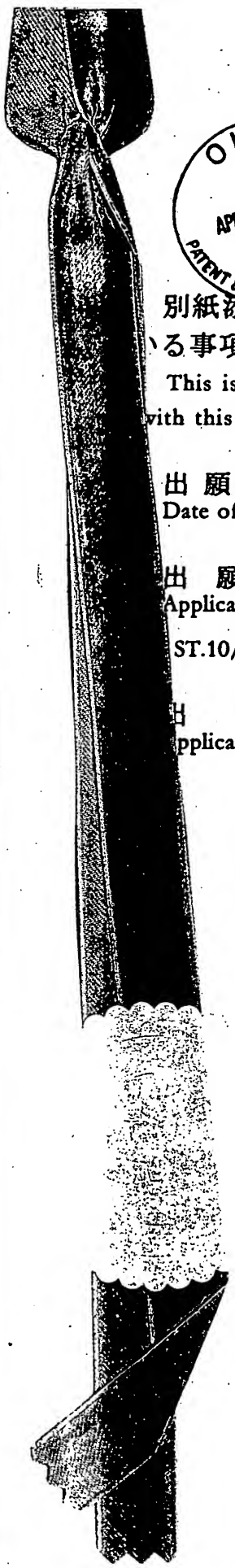


日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００２年 ２月１９日

出 願 番 号
Application Number: 特願２００２－０４１８９０

ST.10/C]: [ＪＰ２００２－０４１８９０]

出 願 人
Applicant(s): 株式会社ソニー・コンピュータエンタテインメント

２００２年 ３月 ８日

特 許 庁 長 官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００２－３０１４５２９

US

【書類名】　特許願

【整理番号】　SCEI01206

【あて先】　特許庁長官殿

【国際特許分類】　G06K　1/00

G06N　1/00

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　島田　宗毅

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　岡本　伸一

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　吉森　正治

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　犬井　努

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　島川　恵三

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　岡田　豊史

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　九保　亮

【発明者】

【住所又は居所】　東京都港区赤坂７丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

【氏名】　中村　光宏

【特許出願人】

【識別番号】　395015319

【氏名又は名称】　株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】　100107238

【弁理士】

【氏名又は名称】　米山　尚志

【先の出願に基づく優先権主張】

【出願番号】　特願2001- 44358

【出願日】　平成13年 2月20日

【手数料の表示】

【予納台帳番号】　111236

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0014358

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法

【特許請求の範囲】

【請求項１】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付され、管理者側からユーザに配布される記憶媒体と、

上記記憶媒体に記憶されているコンテンツを、上記暗号化鍵に対応する復号化鍵を用いて復号化して二次記憶媒体にコピーするコピー機能を有し、該コンテンツのコピーを行う際に、上記記憶媒体の媒体識別情報と共に、所定かつ固有のデバイス識別情報を送信するユーザの端末装置と、

上記記憶媒体の媒体識別番号を受信した際に、上記デバイス識別情報を有するユーザの端末装置に対して、上記コンテンツの復号化鍵を送信する管理サーバ装置と

を有するコピー管理システム。

【請求項２】　請求項１記載のコピー管理システムであって、

上記管理サーバ装置は、一つの媒体識別情報に対して１回のみ復号化鍵の送信を行うこと

を特徴とするコピー管理システム。

【請求項３】　請求項１又は請求項２記載のコピー管理システムであって、

上記端末装置は、上記端末装置の識別情報、上記コンテンツのコピーを行うコピー手段に固有に付された識別情報、及び外付けの半導体メモリに固有に付された識別番号のうち、いずれか１つ或いは複数を組み合わせ、上記デバイス識別情報として送信すること

を特徴とするコピー管理システム。

【請求項４】　請求項１から請求項３のうち、いずれか一項記載のコピー管

理システムであって、

上記管理サーバ装置は、上記デバイス識別情報で上記復号化鍵を暗号化して送信し、

上記端末装置は、自己のデバイス識別情報で、上記暗号化された復号化鍵を復号化して用いること

を特徴とするコピー管理システム。

【請求項５】　請求項１から請求項４のうち、いずれか一項記載のコピー管理システムであって、

上記端末装置は、上記コンテンツの復号化後に、上記復号化鍵を削除すること

を特徴とするコピー管理システム。

【請求項６】　請求項１から請求項５のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信し、

上記端末装置は、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーし、上記再暗号化鍵を記憶手段に記憶し、上記記憶手段に記憶した再暗号化鍵を用いて、上記コピーされたコンテンツを復号化して再生すること

を特徴とするコピー管理システム。

【請求項７】　請求項１から請求項６のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、各ユーザのデバイス識別情報に関連付けして上記復号化鍵を送信済みの媒体識別情報をデータベースに記憶することで上記復号化鍵の配信管理を行い、修理或いは交換によりユーザのデバイス識別情報が変更された場合、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えること

を特徴とするコピー管理システム。

【請求項８】　請求項１から請求項７のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、復号化鍵の送信を行った端末装置を有するユーザに対して所定の課金処理を行うこと

を特徴とするコピー管理システム。

【請求項９】　請求項１から請求項８のうち、いずれか一項記載のコピー管理システムであって、

上記ユーザの端末装置と上記管理サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記復号化鍵をユーザの端末装置に送信した際に、ユーザに対する課金処理を行う仲介サーバ装置を有すること

を特徴とするコピー管理システム。

【請求項１０】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップと

を有するクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項１１】　請求項１０記載の記憶媒体であって、

上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理すること

を特徴とする記憶媒体。

【請求項１２】　請求項１０又は請求項１１記載の記憶媒体であって、

上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有すること

を特徴とする記憶媒体。

【請求項１３】　請求項１０から請求項１２のうち、いずれか一項記載の記憶媒体であって、

上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、

上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、

上記再暗号化鍵を記憶手段に記憶するステップと、

コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップと

を有することを特徴とする記憶媒体。

【請求項１４】　請求項１０から請求項１３のうち、いずれか一項記載の記憶媒体であって、

上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信すること

を特徴とする記憶媒体。

【請求項１５】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと

を有する管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項１６】　請求項１５記載の記憶媒体であって、

上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有すること

を特徴とする記憶媒体。

【請求項１７】　請求項１５又は請求項１６記載の記憶媒体であって、

上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信すること

を特徴とする記憶媒体。

【請求項１８】　請求項１５から請求項１７のうち、いずれか一項記載の記憶媒体であって、

上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信すること

を特徴とする記憶媒体。

【請求項１９】　請求項１５から請求項１８のうち、いずれか一項記載の記憶媒体であって、

修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有すること

を特徴とする記憶媒体。

【請求項２０】　請求項１５から請求項１９のうち、いずれか一項記載の記憶媒体であって、

上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有すること

を特徴とする記憶媒体。

【請求項２１】　請求項１５から請求項２０のうち、いずれか一項記載の記

載の記憶媒体であって、

上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする記憶媒体。

【請求項２２】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップと

を有するクライアント端末装置の情報処理プログラム。

【請求項２３】　請求項２２記載の情報処理プログラムであって、

上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理することを特徴とする情報処理プログラム。

【請求項２４】　請求項２２又は請求項２３記載の情報処理プログラムであって、

上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有すること

を特徴とする情報処理プログラム。

【請求項２５】　請求項２２から請求項２４のうち、いずれか一項記載の情報処理プログラムであって、

上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、

上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、

上記再暗号化鍵を記憶手段に記憶するステップと、

コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップと

を有することを特徴とする情報処理プログラム。

【請求項２６】　請求項２２から請求項２５のうち、いずれか一項記載の情報処理プログラムであって、

上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信すること

を特徴とする情報処理プログラム。

【請求項２７】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップと

を有する管理サーバ装置の情報処理プログラム。

【請求項２８】　請求項２７記載の情報処理プログラムであって、

上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有すること

を特徴とする情報処理プログラム。

【請求項２９】　請求項２７又は請求項２８記載の情報処理プログラムであって、

上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信すること

を特徴とする情報処理プログラム。

【請求項３０】　請求項２７から請求項２９のうち、いずれか一項記載の情報処理プログラムであって、

上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信すること

を特徴とする情報処理プログラム。

【請求項３１】　請求項２７から請求項３０のうち、いずれか一項記載の情報処理プログラムであって、

修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有すること

を特徴とする情報処理プログラム。

【請求項３２】　請求項２７から請求項３１のうち、いずれか一項記載の情報処理プログラムであって、

上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有すること

を特徴とする情報処理プログラム。

【請求項３３】　請求項２７から請求項３２のうち、いずれか一項記載の記載の情報処理プログラムであって、

上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識

別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする情報処理プログラム。

【請求項３４】　固有のデバイス識別番号が付されたユーザのデバイスで、固有の媒体識別情報が付された記憶媒体に暗号化鍵で暗号化されて記憶されているコンテンツのコピーを行う際に、上記デバイスから上記デバイス識別情報及び上記媒体識別情報を管理サーバ装置に送信し、

コンテンツのコピーが行われた記憶媒体の媒体識別情報が、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で登録されるデータベースに、上記ユーザのデバイスから送信された媒体識別情報が登録されているか否かを上記管理サーバ装置が検出し、

上記データベースに、上記媒体識別情報が未登録であった場合に、上記管理サーバ装置からユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する

コピー管理方法。

【請求項３５】　暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出し、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出し、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信し、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信し、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理し、

上記復号化処理したコンテンツをコピーする

クライアント端末装置の情報処理方法。

【請求項３６】　ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信し、

各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出し、

上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する

管理サーバ装置の情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばゲームコンテンツ，映画コンテンツ，音楽コンテンツ，アプリケーションプログラム等のコンピュータプログラムのコピー管理を行うコピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法に関する。

【０００２】

【従来の技術】

今日において、例えばＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ或いは半導体メモリ等の記憶媒体に記憶されているゲームコンテンツに基づいてビデオゲームを実行するビデオゲーム機が広く普及している。

【０００３】

ユーザは、所望のゲームコンテンツが記憶された記憶媒体を購入し、この記憶媒体をビデオゲーム機で再生してビデオゲームを行う。大抵の場合、ユーザは、徐々に新しいビデオゲームを買い揃えていく。このため、月日と共にユーザの手元には各ゲームコンテンツが記憶された記憶媒体が蓄積されていくこととなる。

【０００４】

しかし、ビデオゲーム機には、記憶媒体の再生機構が１基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取り出し、これから行おうとするゲームコンテンツが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。

【０００５】

【発明が解決しようとする課題】

本件出願人は、例えば数十Ｇ（ギガ）オーダーの大容量のハードディスクドライブ（ＨＤＤ）を内蔵或いは外付け可能としたビデオゲーム機を開示している。

【０００６】

このビデオゲーム機の場合、各記憶媒体に記憶されているゲームコンテンツをそれぞれＨＤＤにコピーし、このＨＤＤから所望のゲームコンテンツを再生して利用することができる。このＨＤＤを用いることにより、ビデオゲーム機の再生機構に記憶媒体を着脱する手間を省略することができる。

【０００７】

ここで、ゲームコンテンツ等のコンピュータプログラムは、そのコンピュータプログラムが記憶されたソフトウェアを購入する等して正当に入手したユーザのみが使用可能なはずである。

【０００８】

しかし、記憶媒体に記憶されたコンピュータプログラムを二次記憶媒体にコピー可能とした場合、一つの記憶媒体に記憶されているコンピュータプログラムを、複数のユーザがそれぞれ二次記憶媒体にコピーして使用する不正コピーが懸念される。

【０００９】

本発明は、上述の課題に鑑みてなされたものであり、正当なユーザに対してのみ、コンピュータプログラムのコピーを可能とするコピー管理を行うことで、コンテンツの不正使用の防止等を図ったコピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管

理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法の提供を目的とする。

【００１０】

【課題を解決するための手段】

本発明は、暗号化鍵で暗号化したコンテンツを記憶させた記憶媒体に対して固有の識別番号を付してユーザに配布する。ユーザがコンテンツのコピーを行う際に使用するデバイスにも識別番号が付されている。

【００１１】

上記デバイスは、コンテンツのコピーを行う際に、上記記憶媒体の識別番号、及びデバイスの識別番号を管理サーバ装置に送信する。管理サーバ装置は、各ユーザが使用するデバイスの識別番号が登録されたデータベースを有している。管理サーバ装置は、データベースに登録されているデバイスの識別番号と、ユーザのデバイスから送信されたデバイスの識別番号とを照合してユーザを特定する。管理サーバ装置は、この照合を行うことでユーザが特定された際に、記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザのデバイスに送信する。

【００１２】

ユーザのデバイスは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してコンテンツのコピーを行う。

【００１３】

これにより、記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーを許可することができ、コンテンツの不正コピーを防止することができる。

【００１４】

【発明の実施の形態】

本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

【００１５】

コンピュータプログラムとしては、例えばゲームコンテンツ，音楽コンテンツ，映画コンテンツ，アプリケーションプログラム等がある。また、コンピュータプログラムが記憶された記憶媒体としては、ＤＶＤ－ＲＯＭ，ＣＤ－ＲＯＭ等の光ディスクの他、半導体メモリがある。また、コンピュータプログラムのコピー先となる二次記憶媒体としては、ハードディスク（ＨＤ），ＤＶＤ－ＲＡＭや光磁気ディスク（ＭＯ）等がある。

【００１６】

以下、上記ゲームコンテンツ，音楽コンテンツ，映画コンテンツ，アプリケーションプログラム等を総称して、単に「コンテンツ」ということとする。

【００１７】

［コピー管理システムの全体構成］

まず、図１に本発明の第１の実施の形態となるコピー管理システムの全体構成を示す。この図１に示すように、この第１の実施の形態のコピー管理システムは、光ディスクに記憶されているコンテンツの再生機能（実行機能）、及びネットワークを介した通信機能を備えたクライアント端末装置１を有している。

【００１８】

このクライアント端末装置１には、光ディスクに記憶されたコンテンツをコピーするためのハードディスクドライブ２（ＨＤＤ）が接続されている。

【００１９】

また、このクライアント端末装置１には、インターネット５などのネットワークとの接続を図るための通信モデム６が接続されている。

【００２０】

なお、通信モデム６は、この図１に示すようにクライアント端末装置１に対して外付けのかたちで設けてもよい。また、通信モデム６は、クライアント端末装置１に内蔵のかたちで設けてもよい。

【００２１】

また、コピー管理システムは、ユーザエントリ情報が記憶されたデータベース３を備えたシステムサーバ装置４を有している。

【００２２】

このシステムサーバ装置４と上記クライアント端末装置１とが、例えばインターネット５等のネットワークを介して相互に接続されることでこの第１の実施の形態のコピー管理システムが構成されている。

【００２３】

［クライアント端末装置の構成］

図２に、クライアント端末装置１の外観の斜視図を示す。この図２示すように、クライアント端末装置１の前面側には、コントローラ接続部７Ａ，７Ｂと、メモリカード装着部８Ａ，８Ｂが設けられている。

【００２４】

また、このクライアント端末装置１の前面側には、ＵＳＢ対応機器（ＵＳＢ：Universal Serial Bus）が接続される２つのＵＳＢ接続端子９と、例えば最大４００Ｍｂｐｓのデータ転送速度に対応可能なＩＥＥＥ１３９４接続端子１０とが設けられている。

【００２５】

また、このクライアント端末装置１の前面側には、光ディスクが装着されるトレイ型のディスク装着部１１が設けられている。

【００２６】

また、このクライアント端末装置１の前面側には、コンテンツの実行動作や再生動作をリセットするためのリセットボタン１２と、光ディスク装着部１１のトレイの出し入れを操作するためのトレイ操作ボタン１３とが設けられている。

【００２７】

クライアント端末装置１の背面側には、電源スイッチ、音声映像出力端子（ＡＶマルチ出力端子）、ＰＣカードスロット、光デジタル出力端子、ＡＣ電源入力端子等が設けられている。

【００２８】

ＡＶマルチ出力端子は、ＡＶケーブル１７を介してモニタ用のテレビジョン受像機１８に接続される。クライアント端末装置１から出力される映像信号や音声信号は、このＡＶマルチ出力端子及びＡＶケーブル１７を介してモニタ用のテレビジョン受像機１８に供給される。これにより、上記コンテンツの映像がテレビ

ジョン受像機１８に表示される。また、上記コンテンツの音声がテレビジョン受像機のスピーカ装置を介して発音される。

【００２９】

コントローラ接続部７Ａ、７Ｂには、コントローラケーブル１５を介してそれぞれコントローラ１４が接続される。

【００３０】

メモリカード装着部８Ａ、８Ｂには、ゲームデータのセーブ（記憶）及び読み出しを行うセーブ用のメモリカード等が装着される。

【００３１】

［ハードディスクドライブの構成］

次に、図２において、クライアント端末装置１の上面部に載置されている筐体がハードディスクドライブ２（以下、ＨＤＤ２という）である。このＨＤＤ２は、内部に例えば４０ＧＢ等の大容量のハードディスクが設けられている。このＨＤＤ２には、十数枚分のＤＶＤ－ＲＯＭに記憶されたゲームコンテンツをコピー可能となっている。

【００３２】

ＨＤＤ２の前面側には、電源投入時に点灯駆動される電源ランプ２０と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ２１とが設けられている。ＨＤＤ２の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けられている。

【００３３】

ＨＤＤ２をクライアント端末装置１に接続する場合、クライアント端末装置１の背面側に設けられた上記ＰＣカードスロットにＰＣカードを挿入する。この状態で、ＰＣカードに接続ケーブルの一端を接続する。接続ケーブルの他端は、ＨＤＤ２のデータ入出力端子に接続する。これにより、クライアント端末装置１とＨＤＤ２とが、電気的に相互に接続される。

【００３４】

なお、この例においては、ＨＤＤ２はクライアント端末装置１とは別体で、クライアント端末装置１に対して外付けすることとした。しかし、このＨＤＤ２を

、クライアント端末装置１に内蔵するかたちで設けてもよい。

【００３５】

また、クライアント端末装置１とＨＤＤ２とをＰＣカードと接続ケーブルを介して接続することとした。しかし、ＨＤＤ２の背面側（或いは前面側でもよい。）にＵＳＢ接続端子やＩＥＥＥ１３９４接続端子等の接続端子を設け、この接続端子を介してＨＤＤ２をクライアント端末装置１に接続するようにしてもよい。

【００３６】

［クライアント端末装置の電気的構成］

次に、図３はクライアント端末装置１のブロック図である。この図３に示すように、クライアント端末装置１は、ＣＰＵ３０と、グラフィックプロセツサ３１（ＧＰＵ）と、ＩＯプロセッサ３２（ＩＯＰ）を有している。

【００３７】

また、クライアント端末装置１は、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の光ディスクの再生制御を行う光ディスク制御部３３と、サウンドプロセッサユニット３４（ＳＰＵ）とを有している。

【００３８】

また、クライアント端末装置１は、ＣＰＵ３０やＩＯＰ３２が実行するオペレーティングシステムプログラムが格納されたＭＡＳＫ－ＲＯＭ３５と、ＣＰＵ３０のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能するＲＡＭ３６とを有している。

【００３９】

また、クライアント端末装置１は、光ディスク制御部３３のＲＦアンプ３７を介して供給される光ディスクからの再生出力に対して、例えば誤り訂正処理（ＣＩＲＣ処理）等を施して出力するＣＤ／ＤＶＤＤＳＰ３８を有している。

【００４０】

また、クライアント端末装置１は、光ディスク制御部３３のスピンドルモータの回転制御、光ピックアップのフォーカス／トラッキング制御、ディスクトレーのローディング制御等を行うドライバ３９及びメカコントローラ４０を有している。

【００４１】

また、クライアント端末装置１は、上記ＰＣカードが接続されるカード型コネクタ４１を有している。

【００４２】

これらの各部は、主にバスライン４２，４３等を介してそれぞれ相互に接続されている。

【００４３】

なお、ＤＶＤ－ＲＯＭに記憶された映画コンテンツの再生は、メモリカードに記憶されたＤＶＤドライバソウフトウェアに基づいて行われる。或いは、映画コンテンツの再生は、クライアント端末装置１内に内蔵された半導体メモリ４４（DVD Player ROM）に焼き付けられたＤＶＤドライバソウフトウェアに基づいて行われる。

【００４４】

ＭＡＳＫ－ＲＯＭ３５には、オペレーティングシステムプログラムが記憶されている。ＣＰＵ３０は、このＭＡＳＫ－ＲＯＭ３５に記憶されているオペレーティングシステムプログラムに基づいて、クライアント端末装置１全体の動作を制御する。

【００４５】

また、ＭＡＳＫ－ＲＯＭ３５には、コントローラ接続部７Ａ，７Ｂと、メモリカード装着部８Ａ，８Ｂ、及びカード型コネクタ４１に接続されるコントローラ１４，メモリカード１６及びＨＤＤ２等のハードウェア識別番号（ハードウェアＩＤ）も記憶されている。ＩＯＰ３２は、このＭＡＳＫ－ＲＯＭ３５に記憶されているハードウェアＩＤに基づいて、コントローラ１４，メモリカード１６及びＨＤＤ２等のハードウェアと通信を行い、各接続端子７Ａ，７Ｂ、８Ａ，８Ｂ及びカード型コネクタ４１等に接続されたハードウェアを特定して認識する。

【００４６】

なお、ハードウェアＩＤは、クライアント端末装置１全体で一つのＩＤ、メモリカード１６全体で一つのＩＤ、及びＨＤＤ２全体で一つのＩＤ等のように、いわば各ハードウェアに対して総称的に付されたＩＤを意味している。

【００４７】

これに対して、後述するクライアントＩＤ，ＭＣ－ＩＤ及びＨＤＤ－ＩＤは、各クライアント端末装置１毎、各メモリカード１６毎、及び各ＨＤＤ２毎にそれぞれ付された各ハードウェア固有のＩＤとなっている。

【００４８】

ＧＰＵ３１は、ＣＰＵ３０からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、ＧＰＵ３１は、座標変換等の処理を行うジオメトリトランスファエンジンとしての機能を有している。

【００４９】

このＧＰＵ３１は、例えば光デイスクに記録されているゲームコンテンツがいわゆる３Ｄグラフィックを利用する場合に、三角形状のポリゴンの集合で仮想的な３次元オブジエクトを構成する。そして、ＧＰＵ３１は、この３次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算を行う。すなわち、ＧＰＵ３１は、レンダリングを行う場合における透視変換処理（３次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

【００５０】

また、ＧＰＵ３１は、ＣＰＵ３０からの描画指示に従って、必要に応じてジオメトリトランスファエンジンを利用しながら、フレームバッファに対して描画を行う。そして、この描画した画像に対応するビデオ信号（ｖｉｓｕａｌ　ｏｕｔ）を出力する。

【００５１】

一方、ＳＰＵ３４は、適応予測符号化された音声データを再生するＡＤＰＣＭ復号機能と、サウンドバッファに記憶されている波形データを再生することで、効果音等の音声信号を再生して出力（ａｕｄｉｏ　ｏｕｔ）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を備えている。このＳＰＵ３４は、いわゆるサンプリング音源として動作する。ＳＰＵ３４は、ＣＰＵ３０からの指示により、サウンドバッファに記憶されている波形データに基づき楽音，効果音等の音声信号を発生する。

【００５２】

このようなクライアント端末装置１は、電源が投入されると、ＣＰＵ３０及びＩＯＰ３２が、ＭＡＳＫ－ＲＯＭ３５からＣＰＵ３０用のオペレーティングシステムプログラム及びＩＯＰ３２用のオペレーティングシステムプログラムをそれぞれ読み出す。

【００５３】

ＣＰＵ３０は、ＣＰＵ３０用のオペレーティングシステムプログラムによりクライアント端末装置１の各部を統括的に制御する。

ＩＯＰ３２は、ＩＯＰ３２用のオペレーティングシステムプログラムによりコントローラ１４，メモリカード１６、及びＨＤＤ２等との間のデータの入出力を制御する。

【００５４】

ＣＰＵ３０は、ＣＰＵ３０用のオペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部３３を制御し、光ディスクに記録されているコンテンツを再生制御する。

【００５５】

再生したコンテンツがビデオゲームのゲームコンテンツである場合、ＣＰＵ３０は、ＩＯＰ３２を介してコントローラ１４から受け付けたプレーヤからの指示（コマンド）に従って、ＧＰＵ３１やＳＰＵ３４を制御し、ゲームコンテンツの画像の表示や効果音，楽音等の発声を制御する。

【００５６】

再生したコンテンツが映画コンテンツの場合、ＣＰＵ３０は、ＩＯＰ３２を介してコントローラ１４から受け付けたプレーヤからの指示に従って、ＧＰＵ３１やＳＰＵ３４を制御し、映画コンテンツの映像の表示や音声の発声等を制御する。

【００５７】

［コピー管理動作］

このようなコピー管理システムは、光ディスクに記憶されているコンテンツがＨＤＤ２にコピーされる際に、以下のように管理する。

【００５８】

〔インストーラのインストール〕

まず、このコピー管理システムは、光ディスクに記憶されているコンテンツをＨＤＤ２にコピーする際に、クライアント端末装置１でコピー制御用のアプリケーションプログラム（インストーラ）を実行する必要がある。この例の場合、インストーラは、コンテンツと共に光ディスクに記憶されている。クライアント端末装置１は、コンテンツのコピー行う前にインストーラのインストールを行う。

【００５９】

インストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置１に装着する。クライアント端末装置１のＣＰＵ３０は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ１４の操作に従って光ディスクに記憶されているインストーラを読み出し、これをメモリカード１６或いはＲＡＭ３６に記憶制御する。

【００６０】

このメモリカード１６或いはＲＡＭ３６に記憶されたインストーラは、ユーザが光ディスクに記憶されているコンテンツのコピーを指定した際に、ＣＰＵ３０により実行される。ＣＰＵ３０は、このインストーラを実行することで、コンテンツのコピー制御を行う。

【００６１】

なお、インストーラは、システム業者側でインストーラのみ記憶された光ディスクを製造し、これをユーザに配布するようにしてもよい。

或いは、システム業者側でインストーラが記憶されたメモリカードを製造し、これをユーザに配布するようにしてもよい。この場合、インストーラのインストール作業を省略可能とすることができる。

【００６２】

或いは、インストーラが記憶されたＲＯＭをクライアント端末装置１内に設けてもよい。この場合でも、インストーラのインストール作業を省略可能とすることができる。

【００６３】

〔コンテンツの暗号化〕

光ディスクに記憶されたコンテンツには、図４に示すように各コンテンツ毎に異なる対称鍵（コンテンツキー：Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて暗号化処理が施されている。また、光ディスクには、このように暗号化処理されたコンテンツの他、各光ディスク毎に固有となる「Ｍｅｄｉａ ｕｎｉｑｕｅ ＩＤ（メディアユニークＩＤ：ＭＩＤ）」が記憶されている。

【００６４】

〔ユーザ登録〕

次に、この第１の実施の形態のコピー管理システムにおいては、光ディスクからＨＤＤ２にコンテンツのコピーを行う場合、各メモリカード１６に固有に付された「メモリカードＩＤ（ＭＣ－ＩＤ）」を用いてシステムサーバ装置４にユーザ登録を行う。このユーザ登録が行われない場合には、コンテンツのコピーは許可されない。

【００６５】

図５は、ユーザがシステムサーバ装置４に対してユーザ登録を行うまでの流れを示すフローチャートである。図６は、このユーザ登録によりクライアント端末装置１とシステムサーバ装置４との間で送受信される情報を示す当該コピー管理システムの模式図である。

【００６６】

この図５及び図６を用いてユーザ登録動作を説明する。図５のフローチャートは、ユーザがクライアント端末装置１のメイン電源を投入することでスタートとなる。

【００６７】

ステップＳ１では、ユーザがインターネット５を介して自分のクライアント端末装置１をシステムサーバ装置４に接続する。

【００６８】

具体的には、このクライアント端末装置１には、図１に示したようにインターネット接続用の通信モデム６が接続（或いは内蔵）されている。ユーザによりイ

ンターネット接続が指定されると、図３に示すＣＰＵ３０は、所定のＷＷＷブラウザに基づいて動作し、この通信モデム６を介して当該クライアント端末装置１とシステムサーバ装置４との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップＳ２に進む。

【００６９】

ステップＳ２では、ＣＰＵ３０が、クライアント端末装置１に装着されたメモリカードの識別番号（ＭＣ－ＩＤ），クライアント端末装置１毎に付された固有の識別番号（クライアントＩＤ）及びＨＤＤ２毎に付された固有の識別番号（ＨＤＤ－ＩＤ）をシステムサーバ装置４に送信制御する。

【００７０】

具体的には、システムサーバ装置４とクライアント端末装置１との通信回線が確立されると、ＣＰＵ３０は、クライアント端末装置１，ＨＤＤ２及びメモリカード１６とそれぞれ通信を行う。ＣＰＵ３０は、この通信により、クライアント端末装置１に固有に付された識別番号（クライアントＩＤ）、ＨＤＤ２に固有に付された識別番号（ＨＤＤ－ＩＤ）、及びクライアント端末装置１に装着されたメモリカード１６に固有に付された識別番号（ＭＣ－ＩＤ）をそれぞれ取得する。

【００７１】

ＣＰＵ３０は、これらの識別番号を、図６に示すようにシステムサーバ装置４側に送信する。これにより、このユーザ登録の行程がステップＳ３に進む。

【００７２】

なお、クライアント端末装置１とシステムサーバ装置４との間においては、例えばＳＳＬ（Secure Sockets Layer）等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

【００７３】

また、この例においては、ＣＰＵ３０は、各デバイスと通信を行うことで、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤを取得してシステムサーバ装置４側に送信することとした。しかし、クライアント端末装置１，ＨＤＤ２及びメモリカード１６には、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤがそれぞれ

各筐体にユーザが視認可能なかたちで貼り付けられている。このため、ユーザが、このクライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤを見て、コントローラ１４を操作して手動で各ＩＤの入力を行い、システムサーバ装置４側に送信するようにしてもよい。

【００７４】

次に、ステップＳ３では、システムサーバ装置４が、このユーザから送信されたメモリカードの識別番号（ＭＣ－ＩＤ）が有効なＩＤであるか否かを判別する。このユーザ登録行程は、このステップＳ３において、システムサーバ装置４が、ユーザから送信されたＭＣ－ＩＤが有効なＩＤであると判別した場合にステップＳ４に進み、ユーザから送信されたＭＣ－ＩＤが無効なＩＤであると判別した場合にステップＳ７に進む。

【００７５】

具体的には、システムサーバ装置４は、全てのクライアント端末装置１のクライアントＩＤ，全てのＨＤＤ２のＨＤＤ－ＩＤ、及び全てのメモリカード１６のＭＣ－ＩＤを記憶したデータベース３を有している。

【００７６】

システムサーバ装置４は、ユーザからクライアント端末装置１，ＨＤＤ２及びメモリカード１６の各固有のＩＤが送信されると、まず、ユーザから送信されたメモリカード１６の固有のＩＤであるＭＣ－ＩＤと、データベース３に登録されている各ＭＣ－ＩＤとを照合し、ユーザから送信されたメモリカード１６のＭＣ－ＩＤと同じＭＣ－ＩＤがデータベース３に登録されているか否かを判別する。

【００７７】

すなわち、システムサーバ装置４は、ユーザから送信されたメモリカード１６のＭＣ－ＩＤは、データベース３に正規に登録されているＭＣ－ＩＤと同じであるか否かを判別する。

【００７８】

ユーザから送信されたメモリカード１６のＭＣ－ＩＤが、データベース３に正規に登録されているいずれのＭＣ－ＩＤとも一致しなかった場合には、システムサーバ装置４は、このユーザ登録のアクセスを、不正なユーザ登録のアクセスと

判断する。この場合、システムサーバ装置４は、ステップＳ７において、例えば「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

【００７９】

一方、ユーザから送信されたメモリカード１６のＭＣ－ＩＤが、データベース３に正規に登録されているいずれかのＭＣ－ＩＤと一致した場合、システムサーバ装置４は、ステップＳ４において、現在、システムサーバ装置４にアクセスしているユーザの固有のＩＤであるユーザＩＤ（Ｕｓｅｒ　ＩＤ）を、例えば乱数等を用いて形成する。

【００８０】

そして、システムサーバ装置４は、図６に示すようにそのユーザのクライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤと共に、上記ユーザの固有のＩＤであるユーザＩＤ（Ｕｓｅｒ　ＩＤ）、及び後に説明するＭＣ－Ｋｅｙを一纏めにし、これを「ユーザエントリ情報」としてシステムサーバ装置４のデータベース３に登録する。

【００８１】

このように、当該実施の形態のコピー管理システムは、各ユーザが所有するクライアント端末装置１，ＨＤＤ２及びメモリカード１６の３つのＩＤの組み合わせで各ユーザを特定してデータベース３に登録する。

【００８２】

クライアント端末装置１，ＨＤＤ２及びメモリカード１６の３つのＩＤが、異なるユーザ間で全て一致するということは有り得ないため、この３つのＩＤに基づいてユーザ登録を行うことにより、ユーザを確実に特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正コピーを、より強力に防止することができる。

【００８３】

なお、ユーザ登録の際に、「ＭＣ－ＩＤのみ」、「クライアントＩＤのみ」、

「ＨＤＤ－ＩＤのみ」、「ＭＣ－ＩＤとクライアントＩＤ」、「ＭＣ－ＩＤとＨＤＤ－ＩＤ」、或いは「クライアントＩＤとＨＤＤ－ＩＤ」をシステムサーバ装置４側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各ＩＤはそれぞれ固有のＩＤであるため、異なるユーザ間で重複することはなく、ユーザを略々確実に特定してユーザ登録を行うことができる。

【００８４】

次に、ユーザ登録の行程がステップＳ５に進むと、システムサーバ装置４は、ユーザ登録が正規に完了した証として、上記ステップＳ４で形成したユーザエントリ情報のうち、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）をＭＣ－Ｋｅｙで暗号化し、これをクライアント端末装置１側に返信する。

【００８５】

〔ＭＣ－Ｋｅｙ〕

ここで、上記「ＭＣ－Ｋｅｙ」は、クライアント端末装置１とシステムサーバ装置４との間で送受信する情報を暗号化するための鍵情報である。このＭＣ－Ｋｅｙは、ＭＣ－ＩＤと共にメモリカード１６内に予め記憶されている。

【００８６】

ＭＣ－ＩＤは、ユーザが視認可能なようにメモリカード１６の筐体に張り付けられているのであるが、このＭＣ－Ｋｅｙはユーザが視認できないようにメモリカード１６内に記憶されている。また、このＭＣ－Ｋｅｙは、ユーザがメモリカード１６内に記憶されている情報を再生した場合でも、表示や出力が行われることのない秘密性の高い情報となっている。このため、このＭＣ－Ｋｅｙは、ユーザレベルでは、認識することはできないようになっている。

【００８７】

また、システムサーバ装置４のデータベース３には、全てのメモリカード１６のＭＣ－ＩＤと共に、各メモリカード１６に記憶されたＭＣ－Ｋｅｙが記憶されている。システムサーバ装置４は、ＭＣ－Ｋｅｙが必要となったときに、このデータベース３からＭＣ－Ｋｅｙを読み出して参照する。このため、クライアント端末装置１からシステムサーバ装置４に対してＭＣ－Ｋｅｙが送信されることはない。

【００８８】

このように、ＭＣ－Ｋｅｙは、ユーザレベルでは認識することができず、また、クライアント端末装置１とシステムサーバ装置４との間で送受信されることの無い、秘密性の高い情報となっている。

【００８９】

クライアント端末装置１とシステムサーバ装置４との間におけるＭＣ－Ｋｅｙの送受信を不要とすることで、ＭＣ－Ｋｅｙが第三者に傍受される不都合を防止することができる。

【００９０】

システムサーバ装置４は、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）を返信する際、予めデータベース３に記憶されているＭＣ－Ｋｅｙの中から、現在アクセスされているユーザのメモリカード１６に対応するＭＣ－Ｋｅｙを選択する。そして、この選択したＭＣ－Ｋｅｙを用いてユーザＩＤ（Ｕｓｅｒ　ＩＤ）を暗号化してクライアント端末装置１に返信する。

【００９１】

このＭＣ－Ｋｅｙは、上記ユーザＩＤ（Ｕｓｅｒ　ＩＤ），メディアユニークＩＤ（ｍｅｄｉａ　ｕｎｉｑｕｅ　ＩＤ（ＭＩＤ）），コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）、及びＣｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙをそれぞれ復号化する際に用いられる。

【００９２】

ＭＩＤは、各光ディスク毎に固有に付されているＩＤである。コンテンツキーは、光ディスクに記録されたコンテンツを暗号化処理する際に用いられた暗号鍵である。Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙは、ＨＤＤ２にコピーされるコンテンツに対して再暗号化処理を施す際に用いられる暗号鍵である。

【００９３】

クライアント端末装置１は、光ディスクから再生したコンテンツを、上記コンテンツキーを用いて復号化する。そして、クライアント端末装置１は、この復号化したコンテンツを、上記Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙを用いて再暗号化処理してＨＤＤ２にコピーするようになっている。詳しくは後述する。

【００９４】

次に、ユーザ登録行程がステップＳ６に進むと、クライアント端末装置１が、システムサーバ装置４側から返信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）をメモリカード１６に記憶制御する。これにより、この図５のフローチャートに示すユーザ登録の全行程が終了する。そして、この時点において、メモリカード１６には、図６に示すように予め記憶されているＭＣ－ＩＤ及びＭＣ－Ｋｅｙと共に、ＭＣ－Ｋｅｙで暗号化されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）が記憶されることとなる。

【００９５】

〔メディアユニークＩＤの登録とコンテンツキーの取得〕

次に、光ディスクに記録されているコンテンツを何回でもＨＤＤ２にコピー可能とすると、ＭＣ－ＩＤ，ＭＣ－Ｋｅｙ及びユーザＩＤ（Ｕｓｅｒ　ＩＤ）が記録されたメモリカード１６を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているコンテンツをこの他のユーザのＨＤＤに不正にコピーすることが可能となり好ましいことではない。

【００９６】

このコピー管理システムの場合、コンテンツをＨＤＤ２にコピーする際、ユーザがクライアント端末装置１を介して各光ディスク毎に付された固有のメディアユニークＩＤ（ｍｅｄｉａ　ｕｎｉｑｕｅ　ＩＤ（ＭＩＤ））をシステムサーバ装置４側に送信する。システムサーバ装置４は、ユーザから送信されたメディアユニークＩＤを登録すると共に、暗号化されたコンテンツを復号化するためのコンテンツキーをユーザに送信する。クライアント端末装置１は、光ディスクに記録されているコンテンツを、コンテンツキーを用いて復号化してＨＤＤ２にコピーする。このため、このコンテンツキーを受信するということは、システムサーバ装置４からクライアント端末装置１に対して、コンテンツのコピーが許諾されたことを意味する。

【００９７】

システムサーバ装置４は、クライアント端末装置１から受信したメディアユニークＩＤに対して、過去にコンテンツキーの送信が行われていないことを確認し

たうえで、コンテンツキーの送信を行う。これにより、同じメディアユニークＩＤに対するコンテンツキーの送信を、１回のみに制限することができる。

【００９８】

例えば、あるユーザが自分で購入した光ディスクに記憶されているコンテンツを、自分のＨＤＤ２にコピーした後に、この光ディスクを他のユーザに貸与したとする。他のユーザは、ＨＤＤ２にコンテンツをコピーする際に、貸与された光ディスクのメディアユニークＩＤをシステムサーバ装置４に送信する。

【００９９】

しかし、システムサーバ装置４側には、その光ディスクのメディアユニークＩＤに対して、コンテンツキーの送信が行われたことを示す履歴が残っている。この場合、システムサーバ装置４は、他のユーザに対してコンテンツキーの配信は行わない。コンテンツキーを入手することができない他のユーザは、コンテンツをＨＤＤ２にコピーすることはできない。このコピー管理システムは、このようにしてコンテンツの不正コピーを防止している。

【０１００】

図７のフローチャートに、メディアユニークＩＤ（ＭＩＤ）の登録とユーザがコンテンツキーを取得するまでの流れを示す。また、図８に、メディアユニークＩＤの登録の際、及びコンテンツキーの取得の際に、クライアント端末装置１とシステムサーバ装置４との間で送受信される各情報を示す。

【０１０１】

この図７及び図８を用いてメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキーの取得動作を説明する。この図７のフローチャートに示すメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキーの取得行程（登録取得行程）は、ユーザが前述のユーザ登録を正規に終了させていることを前提として実行される。

【０１０２】

まず、ステップＳ１１では、クライアント端末装置１が、システムサーバ装置４との間の通信回線の確立を図る。これにより、この登録取得行程がステップＳ１２に進む。

【０１０３】

なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置１とシステムサーバ装置４との間で確立された通信回線を一旦切断し、この登録取得行程の実行時に、再度、クライアント端末装置１とシステムサーバ装置４との間の通信回線を確立する説明となっている。

【０１０４】

しかし、前述のユーザ登録に続けて、クライアント端末装置１とシステムサーバ装置４との間で確立された通信回線を切断することなく、この登録取得行程を実行するようにしてもよい。この場合、この登録取得行程は、ステップＳ１１をスキップして、スタートからステップＳ１２に進むこととなる。

【０１０５】

次にステップＳ１２では、クライアント端末装置１が、前述のように取得したユーザＩＤ（Ｕｓｅｒ　ＩＤ）及びＭＣ－ＩＤをシステムサーバ装置４に送信する。また、クライアント端末装置１は、このユーザＩＤ及びＭＣ－ＩＤと共に、これからＨＤＤ２にコピーするコンテンツが記憶された光ディスクに対して固有に付されているメディアユニークＩＤ（ＭＩＤ）をシステムサーバ装置４側に送信する。

【０１０６】

具体的には、ＣＰＵ３０は、メモリカード１６と通信を行い、図８に示すようにＭＣ－ＩＤをシステムサーバ装置４側に送信する。また、ＣＰＵ３０は、前述のようにＭＣ－Ｋｅｙで暗号化されたユーザＩＤをメモリカード１６から読み出してシステムサーバ装置４側に送信する。また、ＣＰＵ３０は、光ディスク制御部３３を制御して光ディスクから再生したメディアユニークＩＤ（ＭＩＤ）をＭＣ－Ｋｅｙで暗号化し、これをシステムサーバ装置４側に送信する。

【０１０７】

なお、これらの各情報と共に、クライアントＩＤ及びＨＤＤ－ＩＤをシステムサーバ装置４側に送信するようにしてもよい。クライアントＩＤ及びＨＤＤ－ＩＤは、上記ＭＣ－ＩＤと共にユーザの特定に用いることができる。ＭＣ－ＩＤ，クライアントＩＤ及びＨＤＤ－ＩＤの３つのＩＤを用いてユーザを特定することで、ＭＣ－ＩＤのみでユーザの特定を行う場合よりも、より正確にユーザを特定

することができる。

【０１０８】

また、クライアント端末装置１とシステムサーバ装置４との間で送受信される情報は、例えばＳＳＬ（Secure Sockets Layer）等の通信プロトコルに基づいて暗号化されて送受信される。これにより、クライアント端末装置１とシステムサーバ装置４との間では、安全性の高い通信を行うことができる。

【０１０９】

次に、ステップＳ１３では、システムサーバ装置４が、クライアント端末装置１側から送信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）が有効なＩＤであるか否かを判別する。このステップＳ１３において、システムサーバ装置４が、ユーザＩＤは有効であると判別した場合、この登録取得行程がステップＳ１４に進む。これに対して、このステップＳ１３において、システムサーバ装置４が、ユーザＩＤは無効であると判別した場合、この登録取得行程はステップＳ１７に進む。

【０１１０】

具体的には、システムサーバ装置４は、クライアント端末装置１側から送信されたＭＣ－ＩＤ（及びクライアントＩＤ，ＨＤＤ－ＩＤ）に基づいてデータベース３を参照し、このＭＣ－ＩＤに対応するＭＣ－Ｋｅｙを読み出す。そして、システムサーバ装置４は、このＭＣ－Ｋｅｙに基づいて、ＭＣ－Ｋｅｙで暗号化されて送信されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）及びメディアユニークＩＤ（ＭＩＤ）をそれぞれ復号化する。

【０１１１】

前述のように、システムサーバ装置４側のデータベース３には、ユーザエントリ情報としてユーザＩＤ（Ｕｓｅｒ　ＩＤ），ＭＣ－ＩＤ，クライアントＩＤ及びＨＤＤ－ＩＤ等が記憶されている。このため、システムサーバ装置４は、ＭＣ－ＩＤ（クライアントＩＤ及びＨＤＤ－ＩＤ）に基づいてデータベース３内のユーザ情報を検索する。そして、システムサーバ装置４は、このユーザ情報内のユーザＩＤ（Ｕｓｅｒ　ＩＤ）と、現在システムサーバ装置４側にアクセスしてきているユーザのユーザＩＤ（Ｕｓｅｒ　ＩＤ）とを照合する。

システムサーバ装置４は、上記両者が一致した場合には、現在システムサーバ装

置４側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、この登録取得行程がステップＳ１４に進む。

【０１１２】

これに対して、システムサーバ装置４は、データベース３のユーザ情報内のユーザＩＤ（Ｕｓｅｒ　ＩＤ）と、現在システムサーバ装置４側にアクセスしてきているユーザのユーザＩＤ（Ｕｓｅｒ　ＩＤ）とが不一致の場合、そのユーザＩＤ（Ｕｓｅｒ　ＩＤ）は無効と判断する。そして、システムサーバ装置４は、ステップＳ１７において、例えば「ユーザＩＤが無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【０１１３】

次に、ステップＳ１４では、システムサーバ装置４が、現在アクセスしてきているユーザの光ディスクに記録されているコンテンツは、過去にコピーされた履歴があるか否かを判別する。

【０１１４】

具体的には、このコピー管理システムの場合、データベース３に、各光ディスクにそれぞれ付されているメディアユニークＩＤ（ＭＩＤ）が全て登録されている。システムサーバ装置４は、コンテンツのコピーが行われた際に、データベース３のメディアユニークＩＤ（ＭＩＤ）に対してフラグを立てることで、コピーの履歴を残すようになっている。

【０１１５】

このため、システムサーバ装置４は、メディアユニークＩＤ（ＭＩＤ）を復号化すると、そのメディアユニークＩＤ（ＭＩＤ）に対してフラグが立っているか否かを検出する。これにより、そのメディアユニークＩＤ（ＭＩＤ）を有する光ディスクから過去にコンテンツのコピーが行われたか否かを判別することができる。

【０１１６】

そのメディアユニークＩＤ（ＭＩＤ）のフラグが立っていない場合、そのメデ

ィアユニークＩＤ（ＭＩＤ）が付された光ディスクから過去にコンテンツのコピーは行われていないことを意味する。このため、システムサーバ装置４は、データベース３内におけるそのメディアユニークＩＤ（ＭＩＤ）のフラグを立てる。また、システムサーバ装置４は、このフラグを立てたメディアユニークＩＤ（ＭＩＤ）を、そのユーザのユーザエントリ情報に登録して、この登録取得行程をステップＳ１５に進める。

【０１１７】

これに対して、そのメディアユニークＩＤ（ＭＩＤ）のフラグが立っている場合、過去にそのメディアユニークＩＤ（ＭＩＤ）が付された光ディスクからコンテンツのコピーが行われていることを意味する。このため、システムサーバ装置４は、ステップＳ１７において、例えば「このメディアからコンテンツのコピーをすることはできません。」等のコンテンツのコピーを拒否するメッセージをクライアント端末装置１側に返信する（無効通知）。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【０１１８】

次にステップＳ１５は、過去に、そのユーザの光ディスクからコンテンツのコピーが行われていない場合に進むステップである。この場合、システムサーバ装置４は、そのユーザのメモリカード１６のＭＣ－Ｋｅｙを用いて、光ディスクに記録されているコンテンツを暗号化したコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の暗号化を行う。そして、この暗号化したコンテンツキーをクライアント端末装置１側に送信する。このコンテンツキーの送信は、システムサーバ装置４側からユーザに対して、光ディスクに記録されているコンテンツのコピーが許可されたことを意味する。

【０１１９】

ＭＣ－Ｋｅｙは、そのユーザが所有するメモリカード１６に対して固有に付されている。このため、このコンテンツキーを復号化して使用することができるユーザを、そのＭＣ－Ｋｅｙが記憶されたメモリカード１６を有するユーザのみに限定することができる。従って、上記コンテンツキーを正規のユーザに対してのみ、安全に送信することができる。

【０１２０】

また、システムサーバ装置４は、データベース３に記憶されているユーザエントリ情報に基づいて、そのユーザが使用しているクライアント端末装置１のクライアントＩＤ及びＨＤＤ２のＨＤＤ－ＩＤを読み出す。システムサーバ装置４は、これら各ＩＤを、例えば乱数を用いて形成した「コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）」で暗号化してクライアント端末装置１側に返信する。

【０１２１】

さらに、システムサーバ装置４は、クライアントＩＤ及びＨＤＤ－ＩＤを暗号化する際に用いたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を、上記ＭＣ－Ｋｅｙで暗号化してクライアント端末装置１側に返信する。

【０１２２】

後に説明するが、クライアント端末装置１は、システムサーバ装置４から返信されたクライアントＩＤと、当該クライアント端末装置１のクライアントＩＤとを照合する。また、クライアント端末装置１は、システムサーバ装置４から送信されたＨＤＤ－ＩＤと、当該クライアント端末装置１に接続されているＨＤＤ２のＨＤＤ－ＩＤとを照合する。そして、クライアント端末装置１は、上記２つのクライアントＩＤと、上記２つのＨＤＤ－ＩＤとが、それぞれ一致することを確認してコンテンツのコピーを行うようになっている。

【０１２３】

このため、システムサーバ装置４からユーザのクライアント端末装置１に対して、予め登録されているクライアントＩＤ及びＨＤＤ－ＩＤを返信することにより、予めデータベース３に登録されているそのユーザのクライアント端末装置１とＨＤＤ２の組み合わせでのみ、コンテンツのコピー可能とすることができる。

【０１２４】

さらに、システムサーバ装置４は、クライアントＩＤ及びＨＤＤ－ＩＤを暗号化したコンテンツジェンキーを、そのユーザが所有するメモリカード１６に固有に付されたＭＣ－Ｋｅｙを用いて暗号化してユーザのクライアント端末装置１に返信する。これにより、コンテンツジェンキーを復号化して使用することができ

るユーザを、そのＭＣ－Ｋｅｙが記憶されたメモリカード１６を有するユーザのみに限定することができる。従って、上記コンテンツジェンキーを正規のユーザに対してのみ、安全に送信することができる。

【０１２５】

次に、ステップＳ１６では、クライアント端末装置１が、システムサーバ装置４側から返信されたＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）、ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）、及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをそれぞれメモリカード１６に記憶制御する。これにより、この図７のフローチャートに示す登録取得行程が終了する。

【０１２６】

このように、このコピー管理システムは、過去にコピー履歴の無いメディアユニークＩＤ（ＭＩＤ）を有する光ディスクに記憶されたコンテンツのみコピーの許可を行う。これにより、各光ディスクに記憶されたコンテンツのコピーを１回に制限することができる。このため、過去にコンテンツのコピーが行われた光ディスクを貸与された第三者は、その貸与された光ディスクからコンテンツのコピーを行うことはできない。従って、１枚の光ディスクから多数のユーザがコンテンツのコピーを行う不正使用を防止することができる。

【０１２７】

［コンテンツのコピー］

次に、ユーザは、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を取得することで、光ディスクに記録されているコンテンツをＨＤＤ２にコピーすることが可能となる。

【０１２８】

図９はこのコピー行程の流れを示すフローチャート、図１０はこのコンテンツのコピーが行われる際に、クライアント端末装置１，ＨＤＤ２及びメモリカード１６の間で取り扱う情報を模式的に示した図である。この図９及び図１０を用いてコンテンツのコピー行程の説明を行う。

【０１２９】

まず、図９のフローチャートは、前述のメディアユニークＩＤの登録を終了し、コンテンツキーを取得したユーザが、クライアント端末装置１を操作してコンテンツのコピーを指定することでスタートとなる。

【０１３０】

ステップＳ２１では、クライアント端末装置１のＩＯＰ３２が、それぞれＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をメモリカード１６から読み出し、これらをＣＰＵ３０に供給する。

【０１３１】

前述のように、ＭＣ－Ｋｅｙは、システムサーバ装置４及びこのクライアント端末装置１でそれぞれ保持している。このため、ＣＰＵ３０は、この保持しているＭＣ－Ｋｅｙを用いて、上記暗号化されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を復号化処理する。そして、ＣＰＵ３０は、この復号化したコンテンツキー及びコンテンツジェンキーをＲＡＭ３６に記憶制御する。これにより、このコピー行程がステップＳ２２に進む。

【０１３２】

ステップＳ２２では、ＩＯＰ３２が、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをメモリカード１６から読み出し、これらをＣＰＵ３０に供給する。ＣＰＵ３０は、先に復号化したコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）を用いてこのクライアントＩＤ及びＨＤＤ－ＩＤを復号化する。

【０１３３】

また、このステップＳ２２では、ＣＰＵ３０が、上記復号化したクライアントＩＤと当該クライアント端末装置１に付されたクライアントＩＤとを照合する。また、ＣＰＵ３０は、上記復号化したＨＤＤ－ＩＤと、当該クライアント端末装置１に接続されたＨＤＤ２のＨＤＤ－ＩＤとを照合する。

【０１３４】

次に、ステップＳ２３では、ＣＰＵ３０が、上記各クライアントＩＤ、及び上記各ＨＤＤ－ＩＤがそれぞれ一致するか否かを判別する。両者が一致する場合はコンテンツのコピーを実行すべくこのコピー行程がステップＳ２４に進む。両者が不一致の場合はこのコピー行程がステップＳ２８に進む。

【０１３５】

メモリカード１６から復号化されたクライアントＩＤ及びＨＤＤ－ＩＤが、そのクライアント端末装置１のクライアントＩＤ及びＨＤＤ－ＩＤと一致しないということは、前述のコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得が、正規のユーザのクライアント端末装置１及びＨＤＤ２に基づいて行われていないことを示す。

【０１３６】

すなわち、この場合、正規ユーザからメモリカード１６を貸与された不正ユーザが、コンテンツのコピーを行おうとしていることを示している。

【０１３７】

このため、ＣＰＵ３０は、例えば「コピーを行うことはできません。」等のコンテンツのコピーを拒否するメッセージをユーザに対して表示制御する。これにより、中断されたかたちでこのコピー行程が終了することとなる。

【０１３８】

次に、ステップＳ２４は、クライアント端末装置１が、上記各クライアントＩＤ及び上記各ＨＤＤ－ＩＤの一致を検出した際に実行するステップである。この場合、ＣＰＵ３０は、光ディスク制御部３３により光ディスクから再生されたコンテンツを、ＲＡＭ３６に記憶されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて復号化する。また、ＣＰＵ３０は、この復号化したコンテンツを、ＲＡＭ３６に記憶されているコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で再暗号化してＨＤＤ２に供給する。

【０１３９】

次に、ステップＳ２５では、ＨＤＤ２が、図１０に示すように上記コンテンツジェンキーで再暗号化されたコンテンツをハードディスクに保存（コピー）する。

【０１４０】

次に、ステップＳ２６ではクライアント端末装置１のＣＰＵ３０がＨＤＤ２と通信を行うことで、コンテンツのコピーが完了したか否かを判別する。コピーが完了していない場合、ＣＰＵ３０は、前述のステップＳ２４及びステップＳ２５の動作を繰り返し実行制御することで、コンテンツのコピーが完了するまでの間、ＨＤＤ２に対してコンテンツの供給を行う。コンテンツのコピーが完了すると、このコピー行程がステップＳ２７に進む。

【０１４１】

ステップＳ２７では、コンテンツのコピーが完了したため、ＩＯＰ３２が、メモリカード１６に記憶されているコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を消去する。これにより、このコピー行程が終了する。

【０１４２】

このように、クライアント端末装置１は、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）で暗号化されて光ディスクに記憶されているコンテンツを、システムサーバ装置４から発行されたコンテンツキーで復号化してＨＤＤ２にコピーする。そして、このコンテンツのコピー後に、メモリカード１６内に記憶されているコンテンツキー（システムサーバ装置４から発行されたコンテンツキー）を消去する。

【０１４３】

前述のように、過去にコンテンツのコピーが行われた光ディスクに対しては、データベース３にコピー履歴が残るため、システムサーバ装置４は、原則的にコンテンツキーの再発行は行わない。このため、一度コンテンツのコピーが行われた光ディスクを貸与された第三者からのコピー申請は、システムサーバ装置４が、上記データベースのコピー履歴に基づいて拒否する。そして、システムサーバ装置４は、この第三者に対しては、コンテンツキーを送信しない。

【０１４４】

上記第三者は、コンテンツキーを取得することができないため、貸与された光ディスクに記憶されているコンテンツを復号化することができない。このため、上記第三者がコンテンツをＨＤＤ等の二次記憶媒体にコピーすることができたと

しても、コンテンツを復号化することができないことから、該コンテンツを使用することができない。従って、このコピー管理システムは、コンテンツの不正使用を防止することができる。

【０１４５】

［コピーされたコンテンツの再生］

次に、このようにＨＤＤ２にコピーされたコンテンツは、ユーザが繰り返し再生して利用することができるようになっている。

【０１４６】

図１１に、ＨＤＤ２に保存されたコンテンツの再生行程の流れを示すフローチャートを示す。また、図１２にこの再生行程において、クライアント端末装置１，ＨＤＤ２及びメモリカード１６の間で取り扱われる情報の模式図を示す。

【０１４７】

図１１のフローチャートは、前述のコンテンツのコピーを正規に終了させたユーザが、コンテンツの再生を指定することでスタートとなる。

【０１４８】

ステップＳ３１では、クライアント端末装置１のＩＯＰ３２が、上記ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をメモリカード１６から読み出し、これをＣＰＵ３０に供給する。ＣＰＵ３０は、このコンテンツジェンキーを、クライアント端末装置１側で保持しているＭＣ－Ｋｅｙを用いて復号化して再生する。

【０１４９】

次に、ステップＳ３２では、ＩＯＰ３２が、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤをメモリカード１６から読み出し、これをＣＰＵ３０に供給する。ＣＰＵ３０は、先に復号化したコンテンツジェンキーを用いて、この暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤを復号化する。

【０１５０】

次に、ステップＳ３３では、ＣＰＵ３０が、当該クライアント端末装置１に付されているクライアントＩＤと、上記コンテンツジェンキーで復号化したクライ

アントＩＤとを照合する。

【０１５１】

また、ＣＰＵ３０は、当該クライアント端末装置１に接続されているＨＤＤ２のＨＤＤ－ＩＤと、上記コンテンツジェンキーで復号化したＨＤＤ－ＩＤとを照合する。

【０１５２】

上記各クライアントＩＤ及び上記各ＨＤＤ－ＩＤが一致しないということは、他のユーザのメモリカード１６，他のユーザのクライアント端末装置１、或いは他のユーザのＨＤＤ２が用いられていることを示す。このため、ＣＰＵ３０は、ステップＳ３５において、例えば「コンテンツを再生することはできません。」等のコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのコンテンツの再生行程が終了することとなる。

【０１５３】

このように、このコピー管理システムにおいては、ＨＤＤ２にコピーされたコンテンツを再生する際にも、クライアントＩＤ及びＨＤＤ－ＩＤの照合を行う。例えば、正規のユーザが所有するメモリカード１６とコンテンツが保存されたＨＤＤ２が、第三者に貸与された場合を考える。第三者は、自分のクライアント端末装置に対して、この貸与されたメモリカード１６とＨＤＤ２を接続して、該ＨＤＤ２内に記憶されているコンテンツの再生を行うこととなる。

【０１５４】

しかし、メモリカード１６内に記憶されているクライアントＩＤは、正規のユーザのクライアントＩＤである。このため、第三者のクライアント端末装置のクライアントＩＤと、メモリカード１６に記憶されているクライアントＩＤとが一致しないことから、第三者のクライアント端末装置において、ＨＤＤ２に記憶されているコンテンツの再生は拒否される。このため、メモリカード１６とＨＤＤ２が貸与された場合でも、ＨＤＤ２にコピーされているコンテンツの使用を防止することができる。

【０１５５】

次に、上記各クライアントＩＤ及び上記各ＨＤＤ２がそれぞれ一致した場合、

ＣＰＵ３０は、先に復号化したコンテンツジェンキーを用いてＨＤＤ２のコンテンツを復号化し、これをＲＡＭ３６に記憶する。これにより、このコンテンツの再生行程が終了する。

【０１５６】

ＲＡＭ３６に記憶されたコンテンツが、例えばビデオゲームのゲームコンテンツであった場合、ＣＰＵ３０は、このゲームコンテンツに基づいて動作する。そして、ＣＰＵ３０は、例えばビデオゲームのキャラクタを表示制御し、効果音やＢＧＭ等を発音制御する。これにより、ユーザは、光ディスクからＨＤＤ２にコピーしたゲームコンテンツに基づいてビデオゲームを楽しむことができる。

【０１５７】

光ディスクからゲームコンテンツを直接的に再生してビデオゲームを行う場合、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要である。しかし、このように各光ディスクに記録されたゲームコンテンツをＨＤＤ２にコピーしておくことにより、新たなビデオゲームを行う毎に必要となっていた光ディスクの着脱作業を省略することができる。このため、新たなビデオゲームをスムーズに開始可能とすることができる。

【０１５８】

なお、光ディスクからコンテンツのコピーが終了した後には、メモリカード１６に記憶されているコンテンツキーが消去されるため、コンテンツの再コピーは行うことができない。しかし、メモリカード１６に記憶されているコンテンツジェンキーは、コピー完了後も消去されることはない。このため、コンテンツジェンキーで暗号化されてＨＤＤ２にコピーされたコンテンツは、このメモリカード１６に記憶されているコンテンツジェンキーを用いて繰り返し復号化して再生可能である。

【０１５９】

［デバイスの修理，交換に対する対応］

次に、このコピー管理システムの場合、システムサーバ装置４は、クライアントＩＤ，ＨＤＤ－ＩＤ，ＭＣ－ＩＤ等（以下、一括してデバイスＩＤという）と、ユーザＩＤとをユーザエントリ情報として一括して管理する。しかし、クライ

アント端末装置１やＨＤＤ２等のデバイスを破損等により交換した場合、この交換したデバイスのデバイスＩＤが、ユーザエントリ情報として登録されているデバイスＩＤとは異なるものとなる。従って、デバイスの交換を行うと、正規のユーザであるにも拘わらず、その交換したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【０１６０】

一方、このコピー管理システムの場合、デバイスＩＤの固有性を確保することでコンテンツの不正使用を防止するようになっている。このため、クライアント端末装置１やＨＤＤ２等のデバイスを修理により復元した場合でも、この修理後のデバイスに対して、修理前に付されていたデバイスＩＤとは異なる新たなデバイスＩＤを付し、修理前のデバイスと修理後のデバイスとを明確に区別して管理することが好ましい。

【０１６１】

ただ、このように修理後のデバイスに対して新たなデバイスＩＤを付すと、前述のデバイスの交換時と同様に、正規のユーザであるにも拘わらず、その修理したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【０１６２】

このコピー管理システムは、デバイスの修理及び交換により新たなデバイスＩＤを用いることで懸念される上記不都合を、以下のように防止している。

【０１６３】

〔クライアント端末装置及びＨＤＤの修理，交換に対する対応〕

図１３に、このコピー管理システムにおけるクライアント端末装置及びＨＤＤの修理，交換に対する対応を説明するための模式図を示す。この図１３中、×印が描かれているクライアント端末装置１或いはＨＤＤ２は、破損したデバイスを示している。

【０１６４】

この図１３において、デバイスが破損した場合、ユーザは、その破損したデバイスを、メモリカード１６と共に、このコピー管理システムを管理する管理者側

のリペアセンターに送付する。

【０１６５】

すなわち、この場合メモリカード１６は破損していないのであるが、メモリカード１６にはコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）やコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたクライアントＩＤ及びＨＤＤ－ＩＤ（以下、各ＩＤを一括してデバイスＩＤという）が記憶されている。このため、デバイスが破損した場合でも、この破損したデバイスと共にメモリカード１６を上記リペアセンターに送付（或いは持ち込み）するようになっている。

【０１６６】

リペアセンターでは、故障したデバイスが送付されると、このデバイスが正常に動作するように修理，交換等すると共に、この修理，交換等したデバイスに対して新たなデバイスＩＤを付与する。

【０１６７】

具体的には、クライアント端末装置１のクライアントＩＤは、例えば上記ハードウェアＩＤやオペレーティングシステムプログラムと共にＭＡＳＫ－ＲＯＭ３５に記憶されている。また、ＨＤＤ２内にも上記ＭＡＳＫ－ＲＯＭ３５と同様のＭＡＳＫ－ＲＯＭが設けられており、ＨＤＤ－ＩＤは、このＭＡＳＫ－ＲＯＭに記憶されている。このため、リペアセンターでは、デバイスの修理を行った場合には、この修理を行う前に設けられていたＭＡＳＫ－ＲＯＭを取り外し、新たなクライアントＩＤ或いはＨＤＤ－ＩＤが記憶されたＭＡＳＫ－ＲＯＭに交換することで、新たなクライアントＩＤ或いはＨＤＤ－ＩＤの付与を行う。

【０１６８】

なお、デバイス自体を新品のデバイスに交換する場合は、この新品のデバイスのＭＡＳＫ－ＲＯＭ内に、故障したデバイスとは異なるデバイスＩＤが記憶されているため、上記修理時のようなＭＡＳＫ－ＲＯＭの交換は行わない。

【０１６９】

次に、リペアセンターのオペレータは、故障したデバイスと共に送付されたメモリカード１６のＭＣ－ＩＤを再生する。オペレータは、リペアセンターに設け

られている端末装置を介して上記システムサーバ装置４のデータベース３にアクセスし、上記メモリカード１６から再生したＭＣ－ＩＤに基づいて、上記データベース３に記憶されているユーザエントリ情報を参照する。そして、オペレータは、端末装置を操作して、このデータベース３に記憶されているユーザエントリ情報のうち、デバイスＩＤを、新たに付与したデバイスＩＤに修正登録する。また、オペレータは、端末装置を介してデータベース３を操作し、コピー済みのコンテンツに対して立てられている上記フラグを降ろす。

【０１７０】

また、オペレータは、端末装置を操作して、メモリカード１６内に記憶されている、ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）と、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたデバイスＩＤ（クライアントＩＤ及びＨＤＤ－ＩＤ）とをそれぞれ消去する。そして、このメモリカード１６を、修理，交換等したデバイスと共にユーザに返送（或いは手渡し）する。

【０１７１】

これにより、ユーザのデバイス（クライアント端末装置１，ＨＤＤ２及びメモリカード１６）の状態は、図５及び図６を用いて説明したユーザ登録行程が終了した直後の状態（＝コンテンツのコピーを行う直前の状態）に戻ることとなる。

【０１７２】

このメモリカード１６とデバイスが返送されたユーザは、図７及び図８を用いて説明したメディアユニークＩＤ（ＭＩＤ）の登録とコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得を再度行うようにクライアント端末装置１を操作する。

【０１７３】

クライアント端末装置１は、ユーザの操作に対応してシステムサーバ装置４にアクセスし、メディアユニークＩＤ（ＭＩＤ）の登録を行う。そして、クライアント端末装置１は、この登録によりシステムサーバ装置４から取得したコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を用いて光ディスクに記憶されているコンテンツをＨＤＤ２に再コピーする。

【０１７４】

これにより、デバイスの修理や交換によりデバイスＩＤを新たに付与した場合でも、正規のユーザであれば、新たなデバイスＩＤに基づいてコンテンツのコピーや再生を実行可能とすることができる。

【０１７５】

また、コピー管理システム側では、修理や交換により復元したデバイスに対して新たなデバイスＩＤを付すことにより、修理前のデバイスと修理後のデバイスとを明確に区別して管理することができる。

【０１７６】

〔メモリカードの破損，紛失に対する対応〕

次に、このコピー管理システムの場合、メモリカード１６の破損、或いは紛失に対しては、以下のように対処する。図１４に、このコピー管理システムにおけるメモリカード１６の破損，紛失に対する対応を説明するための模式図を示す。この図１４中、点線の枠で囲んで示すメモリカード１６が、破損或いは紛失したメモリカード１６を示している。

【０１７７】

メモリカード１６が破損或いは紛失した場合、ユーザは、この図１４に示すように、インターネット５を介してクライアント端末装置１をシステムサーバ装置４に接続し、システムサーバ装置４に対してメモリカードの再発行を申請する。

【０１７８】

この申請がなされるとシステムサーバ装置４は、ユーザＩＤの入力画面データをクライアント端末装置１側に送信する。これにより、ユーザのクライアント端末装置１は、テレビジョン受像機１８にユーザＩＤの入力画面を表示制御する。

【０１７９】

ユーザは、この入力画面に対してユーザＩＤの入力を行う。しかし、この場合、メモリカード１６が破損或いは紛失しているため、メモリカード１６からユーザＩＤ（Ｕｓｅｒ　ＩＤ）を読み出すことはできない。このため、ユーザは、ユーザＩＤが発行された際にメモ帳等に書き写しておいたユーザＩＤを見て、ユーザＩＤの入力を行う。クライアント端末装置１は、この入力されたユーザＩＤをシステムサーバ装置４に送信する。

【０１８０】

次にシステムサーバ装置４は、このユーザから送信されたユーザＩＤに対応するユーザエントリ情報をデータベース３から参照する。これにより、システムサーバ装置４は、破損或いは紛失したメモリカード１６のＭＣ－ＩＤ及びＭＣ－Ｋｅｙと共に、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）やそのメモリカード１６でコピーされたコンテンツ等を認識することができる。

【０１８１】

次に、システムサーバ装置４は、新たなＭＣ－ＩＤを有するメモリカード１６ｎｅｗに対して、新たなＭＣ－Ｋｅｙ（Ｎｅｗ－ＭＣ－Ｋｅｙ）と、このＮｅｗ－ＭＣ－Ｋｅｙで新たに暗号化したコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）と、このコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化したクライアントＩＤ及びＨＤＤ－ＩＤを記録し直す。

また、システムサーバ装置４は、データベース３に記憶されているユーザエントリ情報が、この新たなメモリカード１６Ｎｅｗに対応したユーザエントリ情報となるように、ＭＣ－ＩＤやＭＣ－Ｋｅｙ等の書き換えを行う。

【０１８２】

なお、この場合、メモリカード１６が破損或いは紛失した場合であり、ユーザのクライアント端末装置１及びＨＤＤ２は正常に動作している。このため、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されるクライアントＩＤ及びＨＤＤ－ＩＤとしては、元のデバイスＩＤがそのまま用いられる。

【０１８３】

次に、リペアセンターは、このメモリカード１６ｎｅｗを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置４側ではこのメモリカード１６ｎｅｗ内の各情報の書き換えと共に、データベース３のユーザエントリ情報の書き換えを行っている。このため、送付されたメモリカード１６ｎｅｗを受け取ったユーザは、このメモリカード１６ｎｅｗ，クライアント端末装置１及びＨＤＤ２の組み合わせのシステムを用いて、以前と同様に、コンテンツのコピーや、コピーしたコンテンツの再生等を行うことができる。

【０１８４】

［第１の実施の形態の効果］

以上の説明から明らかなように、この第１の実施の形態のコピー管理システムは、システム管理者が、コンテンツキーで暗号化処理を施したコンテンツを、メディアユニークＩＤ（ＭＩＤ）が付された光ディスクに記憶させてユーザに配布する。

【０１８５】

ユーザは、コンテンツのコピーを行う際に、システムサーバ装置４に対して光ディスクのＭＩＤを送信する。また、ユーザは、自分が使用しているデバイスのデバイスＩＤ（クライアントＩＤ，ＨＤＤ－ＩＤ，ＭＣ－ＩＤ等）をシステムサーバ装置４に送信する。

【０１８６】

システムサーバ装置４は、各ユーザが使用しているデバイスのデバイスＩＤに関連付けて、過去にコンテンツのコピーが行われた光ディスクのＭＩＤをデータベース３に記憶している。

【０１８７】

システムサーバ装置４は、ユーザからコンテンツのコピー申請がなされた際に、ユーザが使用しているデバイスＩＤと光ディスクのＭＩＤ基づいてデータベース３を参照する。システムサーバ装置４は、データベース３内に同じＭＩＤが登録されていないことを条件として、コンテンツを復号化するためのコンテンツキーを、ユーザのクライアント端末装置１に送信する。

【０１８８】

クライアント端末装置１は、このコンテンツキーを用いて光ディスクに記憶されているコンテンツを復号化してＨＤＤ２にコピーする。

【０１８９】

このコピー管理システムは、データベース３内に登録されているＭＩＤと同じＭＩＤを掲示してコピー申請がなされた場合は、上記コンテンツキーの配信は行われない。このため、このコピー管理システムは、コンテンツのコピーを１回に制限することができ、コンテンツの不正コピーを防止することができる。

【０１９０】

［第２の実施の形態］

次に本発明の第２の実施の形態となるコピー管理システムの説明をする。上述の第１の実施の形態のコピー管理システムは、ユーザが自分のクライアント端末装置１をシステム管理者側のシステムサーバ装置４に直接的に接続してユーザ登録を行い、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等を取得してコンテンツのコピーを行うものであった。

【０１９１】

この第２の実施の形態のコピー管理システムは、ユーザのクライアント端末装置１とシステム管理者側のシステムサーバ装置４との間に、第３者が管理する第３者管理サーバ装置が設けられている。ユーザはこの第３者管理サーバ装置を介してコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等の取得を行う。第３者管理サーバ装置は、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）等の提供に対する課金を行う。

【０１９２】

［第２の実施の形態の構成］

図１５に、この第２の実施の形態となるコピー管理システムのシステム構成図を示す。この図１５は、光ディスクからコンテンツをコピーする際にコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を取得する流れを示している。

【０１９３】

この図１５において、システムサーバ装置４と第３者管理サーバ装置５０とは、例えば専用回線や、公衆回線を専用回線のように利用可能なＶＰＮ（Virtual Private Network）等により相互に接続されている。

【０１９４】

また、システムサーバ装置４はインターネット５には接続されておらず、この第３者管理サーバ装置５０がインターネット５に接続されている。このため、ユーザは、システムサーバ装置４に対して直接的にアクセスすることはできず、この第３者管理サーバ装置５０を介して間接的にシステムサーバ装置４にアクセスすることとなる。

【０１９５】

［第２の実施の形態の動作］

次に、この第２の実施の形態のコピー管理システムの動作説明をする。この第２の実施の形態のコピー管理システムの場合、光ディスクからコンテンツのコピーを行おうとするユーザは、インターネット５を介して自分のクライアント端末装置１を第３者管理サーバ装置５０に接続する。そして、ユーザは、クライアント端末装置１を介して、ＭＣ－ＩＤ，ユーザＩＤ（Ｕｓｅｒ　ＩＤ），メディアユニークＩＤ（ＭＩＤ）を第３者管理サーバ装置５０側に送信する。また、ユーザは、クライアント端末装置１を介して、第３者管理サーバ装置５０用のアカウント情報（例えばユーザ名やパスワード等）を第３者管理サーバ装置５０に送信する。

【０１９６】

クライアント端末装置１は、ＭＣ－ＩＤ及びアカウント情報をそのまま第３者管理サーバ装置５０に送信する。また、クライアント端末装置１は、ユーザＩＤ（Ｕｓｅｒ　ＩＤ）及び光ディスクのメディアユニークＩＤ（ＭＩＤ）をＭＣ－Ｋｅｙで暗号化し、これらを第３者管理サーバ装置５０に送信する。

【０１９７】

第３者管理サーバ装置５０は、クライアント端末装置１から送信された各情報のうち、アカウント情報を抽出して取得する。また、第３者管理サーバ装置５０は、専用回線（或いは上記ＶＰＮ）を介してＭＣ－ＩＤ，ＭＣ－Ｋｅｙで暗号化されたユーザＩＤ（Ｕｓｅｒ　ＩＤ）、及びＭＣ－Ｋｅｙで暗号化されたメディアユニークＩＤ（ＭＩＤ）をシステムサーバ装置４に送信する。

【０１９８】

システムサーバ装置４は、このＭＣ－ＩＤ，ユーザＩＤ及びＭＩＤを受信すると、前述と同様に暗号化されて光ディスクに記録されているコンテンツを復号化するためのコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）をＭＣ－Ｋｅｙで暗号化して第３者管理サーバ装置５０に返信する。また、システムサーバ装置４は、コンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）をＭＣ－Ｋｅｙで暗号化して第３者管理サーバ装置５０に返信する。さらにシステムサーバ装置４は、このコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）でユーザのクラ

イアントＩＤ及びＨＤＤ－ＩＤを暗号化して第３者管理サーバ装置５０に返信する。

【０１９９】

第３者管理サーバ装置５０は、このＭＣ－Ｋｅｙで暗号化されたコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ），ＭＣ－Ｋｅｙで暗号化されたコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）、及びコンテンツジェンキー（Ｃｏｎｔｅｎｔ－Ｇｅｎ－Ｋｅｙ）で暗号化されたユーザのクライアントＩＤ，ＨＤＤ－ＩＤを、それぞれインターネット５を介してユーザのクライアント端末装置１に転送する。

【０２００】

第３者管理サーバ装置５０は、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）を提供した代償として、先にクライアント端末装置１から送信された第３者管理サーバ装置５０用のアカウント情報に基づいて、そのユーザに対する課金を行う。

【０２０１】

クライアント端末装置１は、第３者管理サーバ装置５０から送信された上記コンテンツキー，コンテンツジェンキー、クライアントＩＤ、及びＨＤＤ－ＩＤをメモリカード１６に記憶制御して、前述のようにコンテンツのコピー、及びコピーしたコンテンツの再生に用いる。

【０２０２】

第３者管理サーバ装置５０側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第３者管理サーバ装置５０は、コンテンツキーの提供と引き替えに課金した金額をクレジットカード会社に請求して回収する。或いは第３者管理サーバ装置５０は、プリペイドされている残金から課金分の金額を減算して回収する。

【０２０３】

このように回収された金銭は、例えばシステムサーバ装置４の管理者と第３者管理サーバ装置５０の管理者との間において、所定の割合で分配されることとなる。

【０２０４】

［第２の実施の形態の効果］

このようにこの第２の実施の形態のコピー管理システムは、クライアント端末装置１とシステムサーバ装置４との間に第３者管理サーバ装置５０を設けて構成する。ユーザはこの第３者管理サーバ装置５０を介してシステムサーバ装置４にアクセスしてコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の配布を請求する。第３者管理サーバ装置５０は、このコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）をユーザに配布して課金を行う。

【０２０５】

これにより、このコピー管理システムは、第３者（第３者管理サーバ装置５０の管理者）が介在するコピー管理システムという新規なコピー管理システムを提供することができる他、上述の第１の実施の形態のコピー管理システムと同じ効果を得ることができる。

【０２０６】

また、このコピー管理システムは、コンテンツキーをユーザに配布した際に課金を行うことで、光ディスク等を介して、或いは所定のネットワークを介してコンテンツを無償でユーザに配布することができる。

【０２０７】

なお、このコピー管理システムにおいて、光ディスクにＭＩＤを付すことなくユーザに配布し、ユーザからコピーの申請があった際に、システムサーバ装置４或いは第３者管理サーバ装置５０が、そのユーザに対してコンテンツキーを配布して課金を行うようにしてもよい。

【０２０８】

また、この第２の実施の形態のコピー管理システムは、第３者管理サーバ装置５０が課金を行うこととしたが、これは、システムサーバ装置４が課金を行うようにしてもよい。

【０２０９】

最後に、本発明は一例として説明した上述の各実施の形態に限定されることはない。このため、上述の各実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論

である。

【０２１０】

例えば、上述の各実施の形態の説明では、クライアント端末装置１は、デバイス識別情報として、クライアントＩＤ，ＨＤＤ－ＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信することとした。しかし、クライアント端末装置１からクライアントＩＤのみをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からＨＤＤ－ＩＤのみをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からＭＣ－ＩＤのみをシステムサーバ装置４に送信してもよい。

【０２１１】

また、クライアント端末装置１からクライアントＩＤ及びＨＤＤ－ＩＤをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からクライアントＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信してもよい。同様に、クライアント端末装置１からＨＤＤ－ＩＤ及びＭＣ－ＩＤをシステムサーバ装置４に送信してもよい。

【０２１２】

すなわち、上述の各実施の形態のコピー管理システムは、システムサーバ装置４側で、コンテンツのコピーが行われる記憶媒体と、コンテンツのコピーに使用されるデバイスとを関連付けてコピー管理を行うことで不正コピーを防止する。このため、クライアント端末装置１からシステムサーバ装置４に送信されるデバイス識別情報としては、ユーザを特定可能な識別情報であればよい。

【０２１３】

また、上述の各実施の形態の説明では、メモリカード１６を用いることとしたが、このコピー管理システムの場合、必ずしもメモリカード１６は必要としない。メモリカード１６を用いない場合は、メモリカード１６に記憶される上記コンテンツキーやコンテンツジェンキー等は、ＨＤＤ２やクライアント端末装置１に内蔵されているメモリに記憶させればよい。

【０２１４】

【発明の効果】

本発明は、記憶媒体の持ち主である正規のユーザに対してのみ、記憶媒体に記憶されたコンテンツのコピーを許可することができる。このため、記憶媒体に記憶されたコンテンツの不正コピーを防止することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態のコピー管理システムのシステム構成を示すブロック図である。

【図２】

コピー管理システムを構成するクライアント端末装置及びハードディスクドライブ（ＨＤＤ）の外観を示す斜視図である。

【図３】

クライアント端末装置の電気的な構成を示すブロック図である。

【図４】

コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）で暗号化されたデジタルコンテンツが記憶された、このコピー管理システムに用いられる光ディスクを説明するための図である。

【図５】

コピー管理システムにおけるユーザ登録の流れを示すフローチャートである。

【図６】

ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図７】

コピー管理システムにおける、光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録動作と、コンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得動作を示すフローチャートである。

【図８】

光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録時、及びコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模

式図である。

【図９】

コピー管理システムにおけるコピー行程の流れを示すフローチャートである。

【図１０】

コピー実行時にクライアント端末装置，メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

【図１１】

コピー管理システムにおける、ハードディスクドライブにコピーしたデジタルコンテンツの再生動作を示すフローチャートである。

【図１２】

ハードディスクドライブにコピーしたデジタルコンテンツの再生時に、クライアント端末装置，メモリカード及びハードディスクドライブの間で送受信される情報を示す模式図である。

【図１３】

クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するコピー管理システムの対応を説明するための模式図である。

【図１４】

メモリカードの破損或いは紛失に対するコピー管理システムの対応を説明するための模式図である。

【図１５】

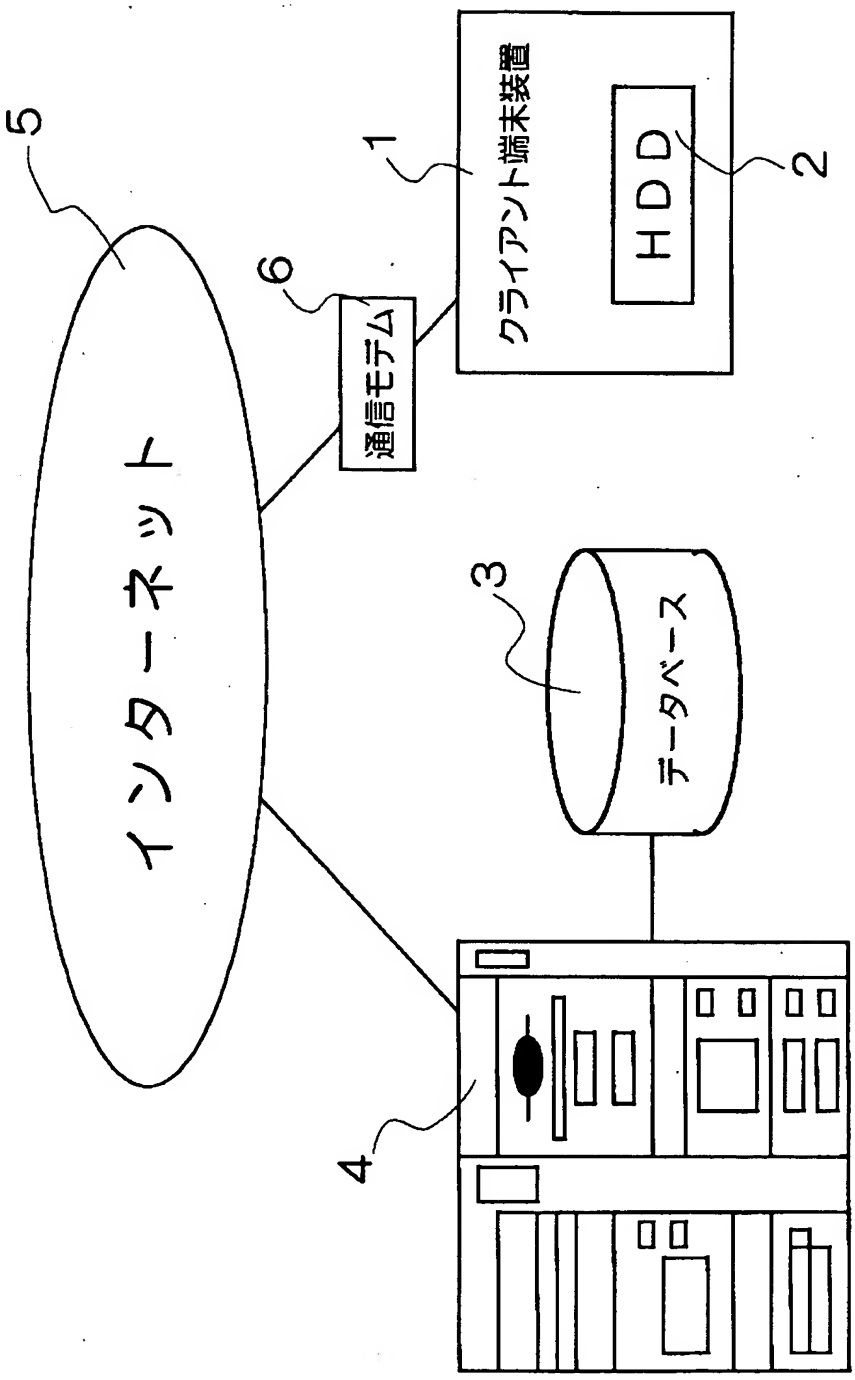
光ディスクに個別に付されたメディアユニークＩＤ（ＭＩＤ）の登録時、及びコンテンツキー（Ｃｏｎｔｅｎｔ－Ｋｅｙ）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第２の実施の形態となるコピー管理システムの模式図である。

【符号の説明】

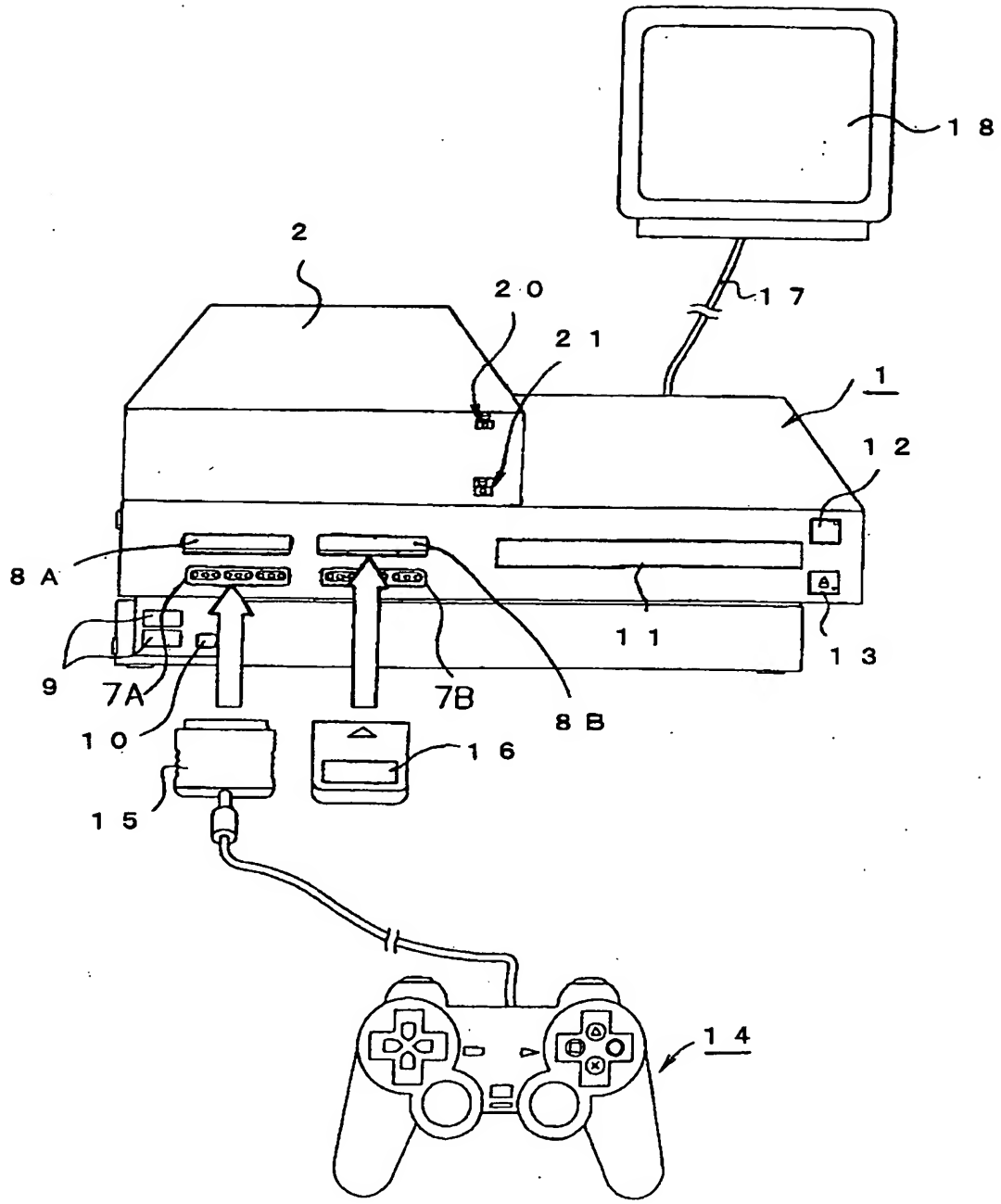
１…クライアント端末装置、２…ハードディスクドライブ（ＨＤＤ），３…データベース，４…システムサーバ装置，５…インターネット，６…通信モデム

【書類名】　　図面

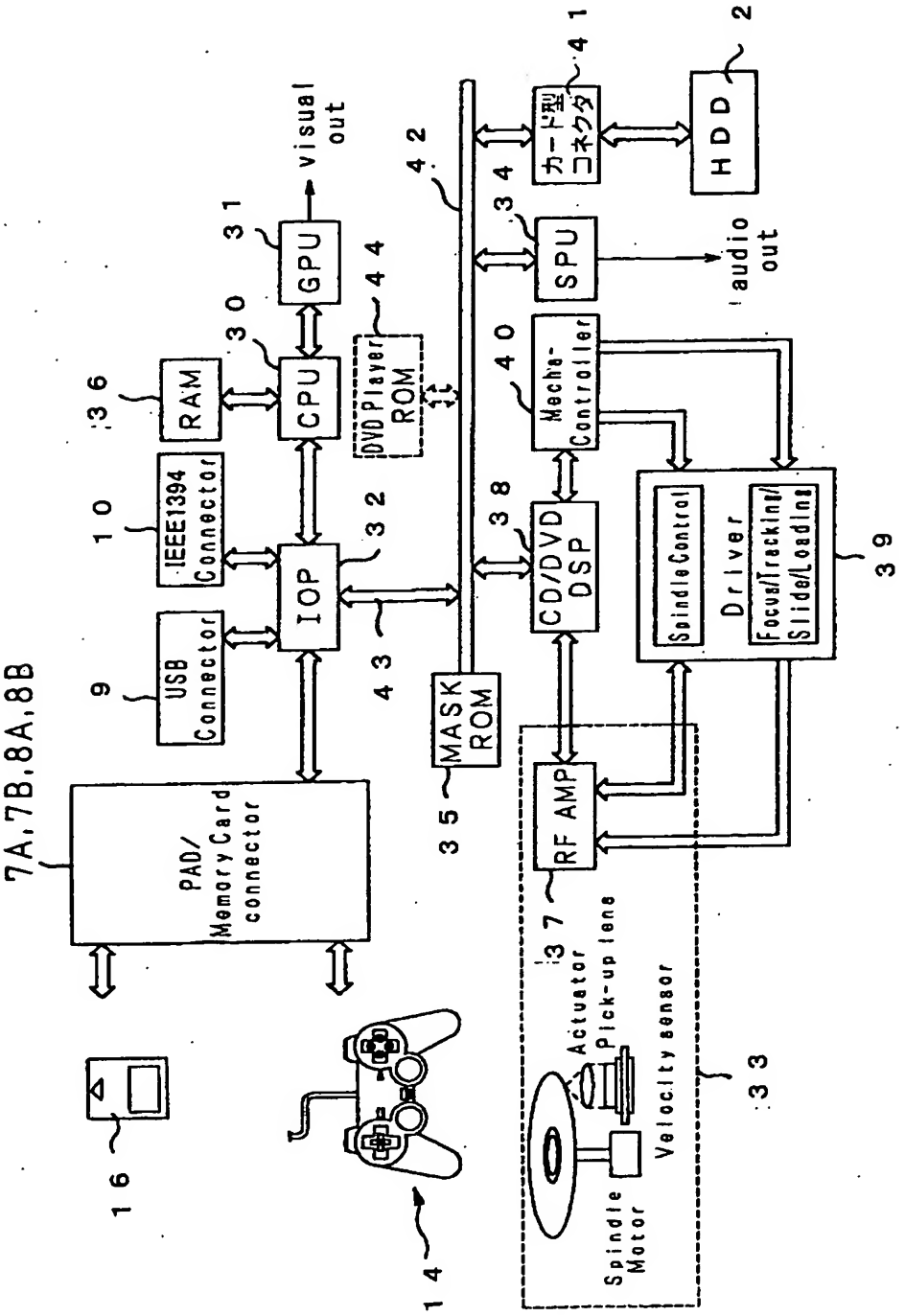
【図１】



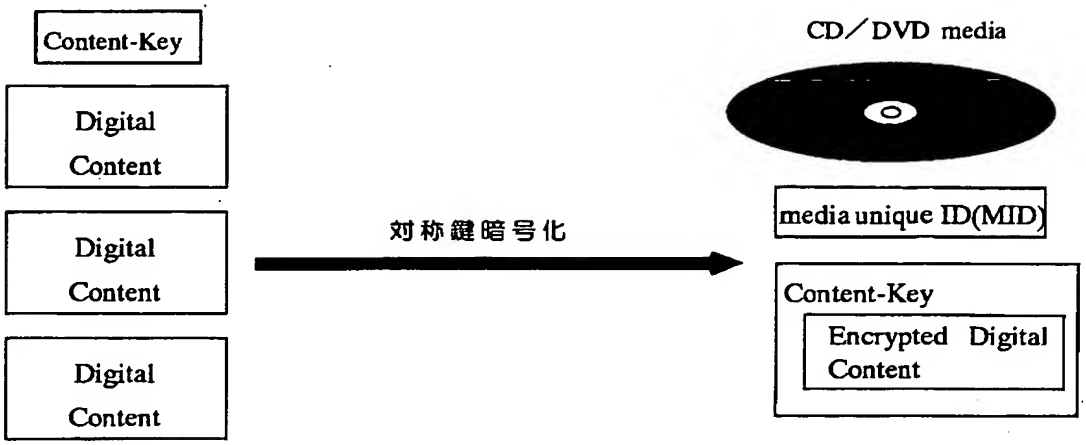
【図２】



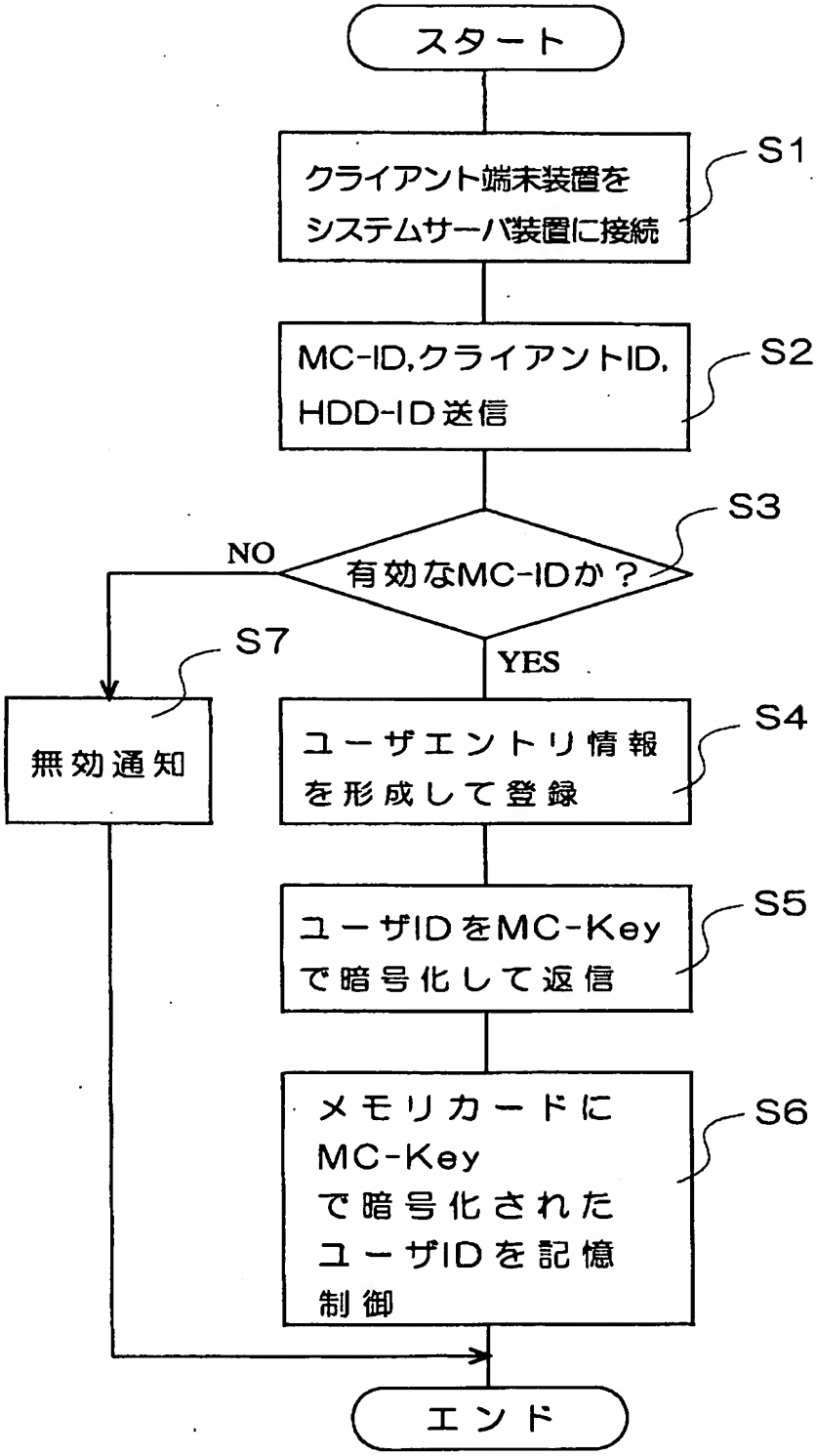
【図３】


visual out
GPU
CPU
RAM
IEEE1394 Connector
USB Connector
IOP
PAD/ MemoryCard connector
7A,7B,8A,8B
DVD Player ROM
MASK ROM
CD/DVD DSP
RF AMP
Actuator
Pick-up lens
Velocity sensor
Spindle Motor
Mecha-Controller
Spindle Control
Driver
Focus/Tracking/ Slide/Loading
SPU
audio out
カード型コネクタ
HDD
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
9
10
14
16

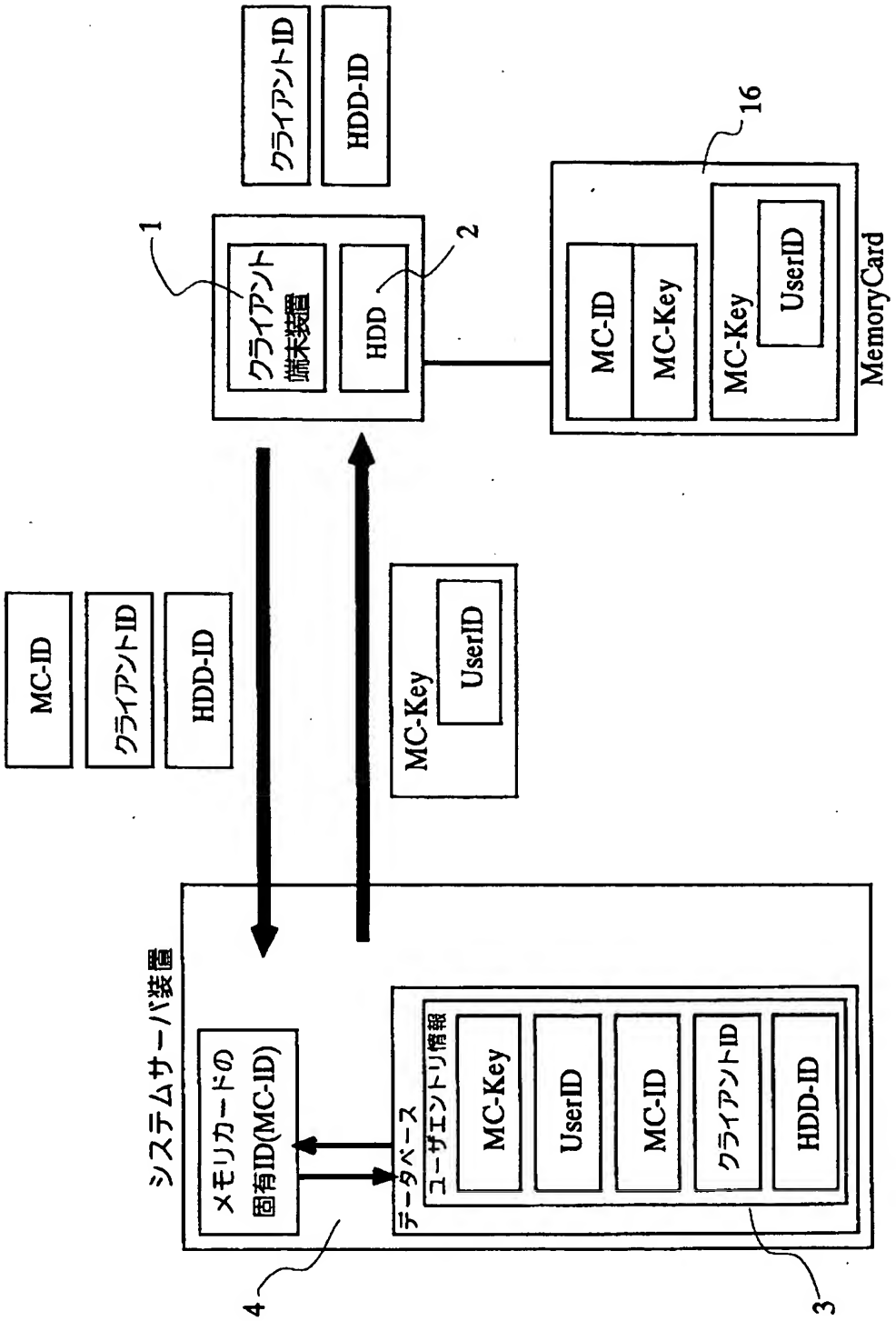
【図４】


Content-Key
Digital Content
Digital Content
Digital Content
対称鍵暗号化
CD／DVD media
media unique ID(MID)
Content-Key
Encrypted Digital Content

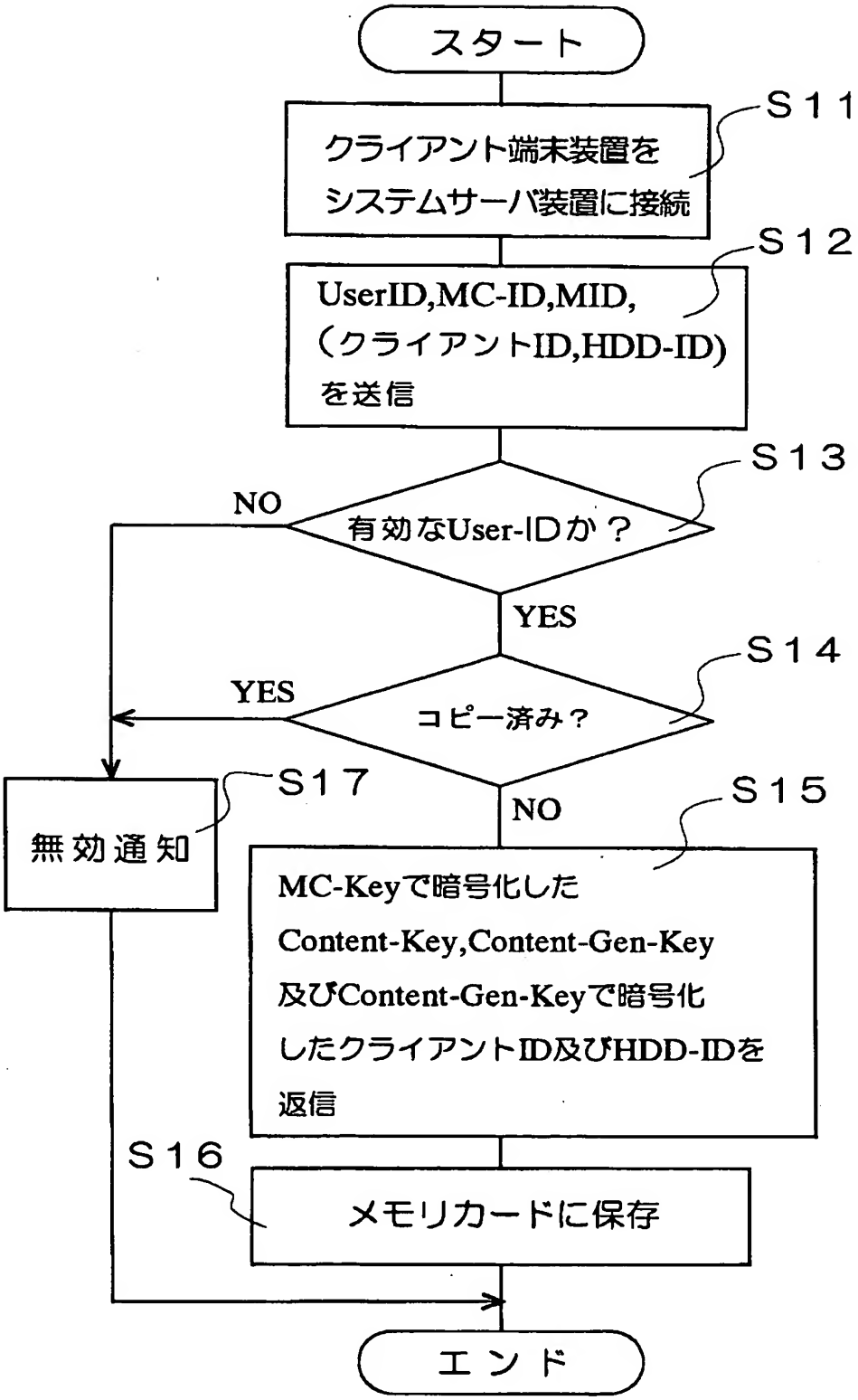
【図５】


スタート
クライアント端末装置を
システムサーバ装置に接続
S1
MC-ID,クライアントID,
HDD-ID送信
S2
有効なMC-IDか？
S3
NO
YES
無効通知
S7
ユーザエントリ情報
を形成して登録
S4
ユーザIDをMC-Key
で暗号化して返信
S5
メモリカードに
MC-Key
で暗号化された
ユーザIDを記憶
制御
S6
エンド

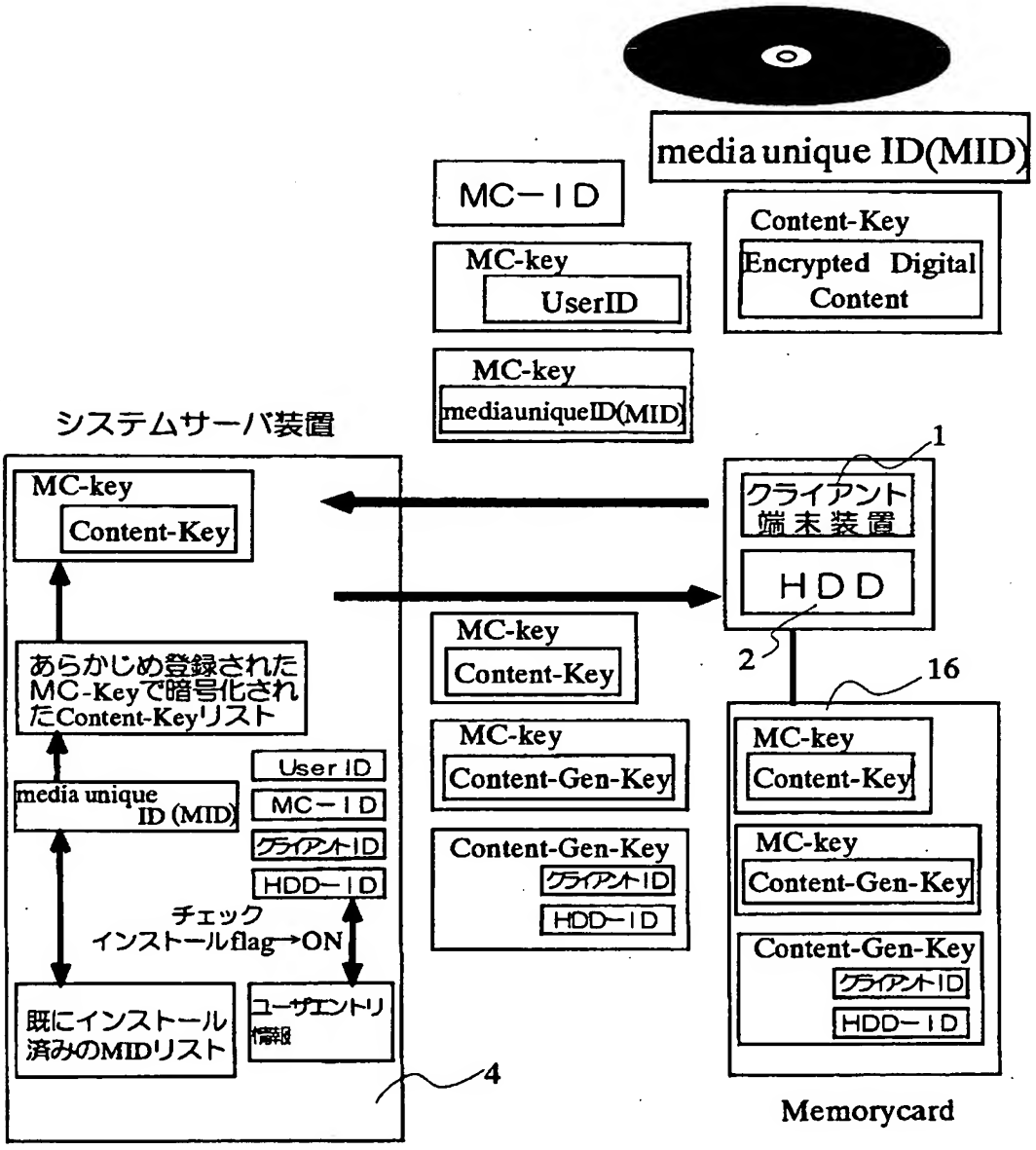
【図６】


クライアントID
HDD-ID
16
1
2
クライアント端末装置
HDD
MC-ID
MC-Key
MC-Key
UserID
MemoryCard
MC-ID
クライアントID
HDD-ID
MC-Key
UserID
システムサーバ装置
メモリカードの固有ID(MC-ID)
データベース
ユーザエントリ情報
MC-Key
UserID
MC-ID
クライアントID
HDD-ID
4
3

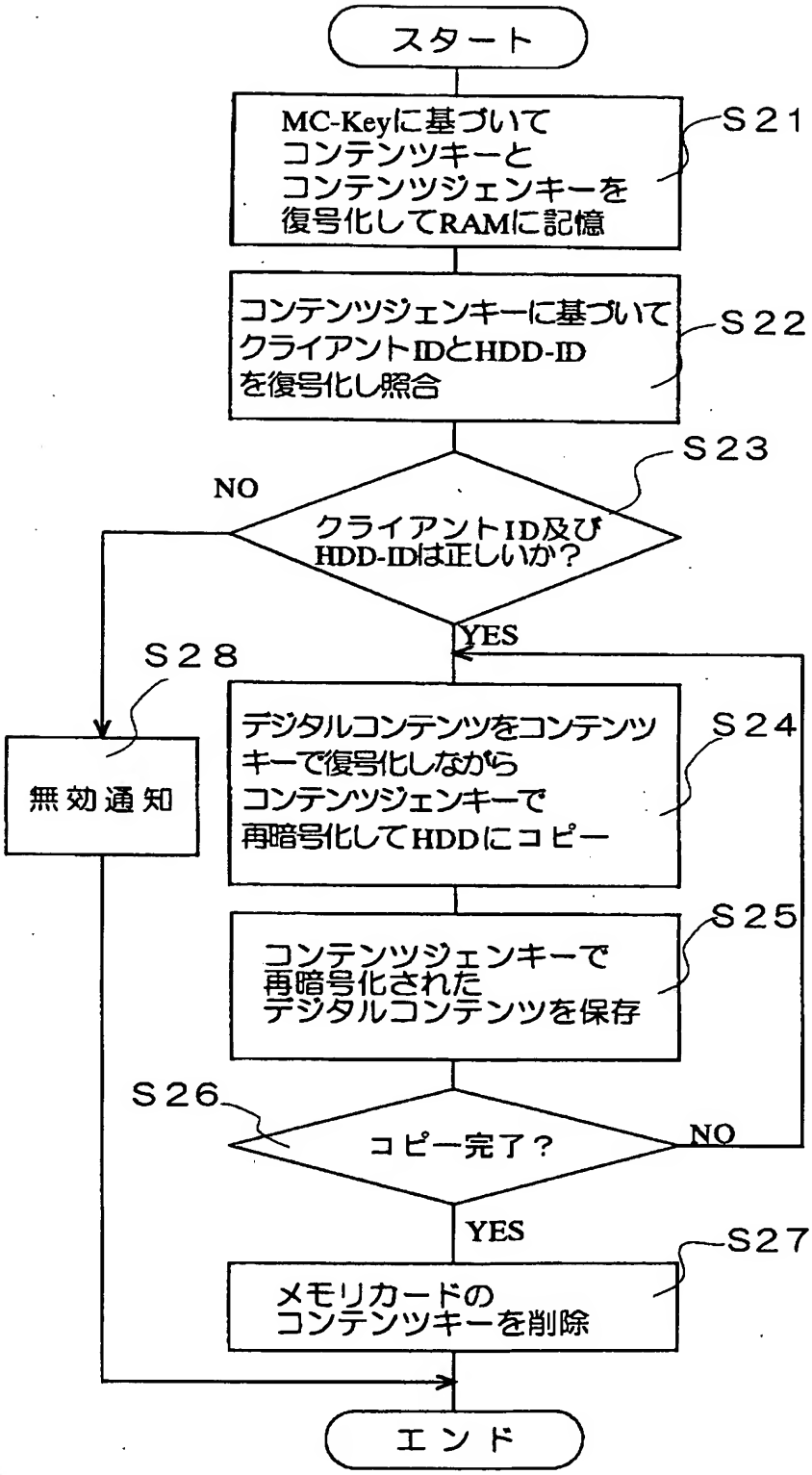
【図７】


スタート
S11
クライアント端末装置を
システムサーバ装置に接続
S12
UserID,MC-ID,MID,
(クライアントID,HDD-ID)
を送信
S13
NO
有効なUser-IDか？
YES
S14
YES
コピー済み？
S17
無効通知
NO
S15
MC-Keyで暗号化した
Content-Key,Content-Gen-Key
及びContent-Gen-Keyで暗号化
したクライアントID及びHDD-IDを
返信
S16
メモリカードに保存
エンド

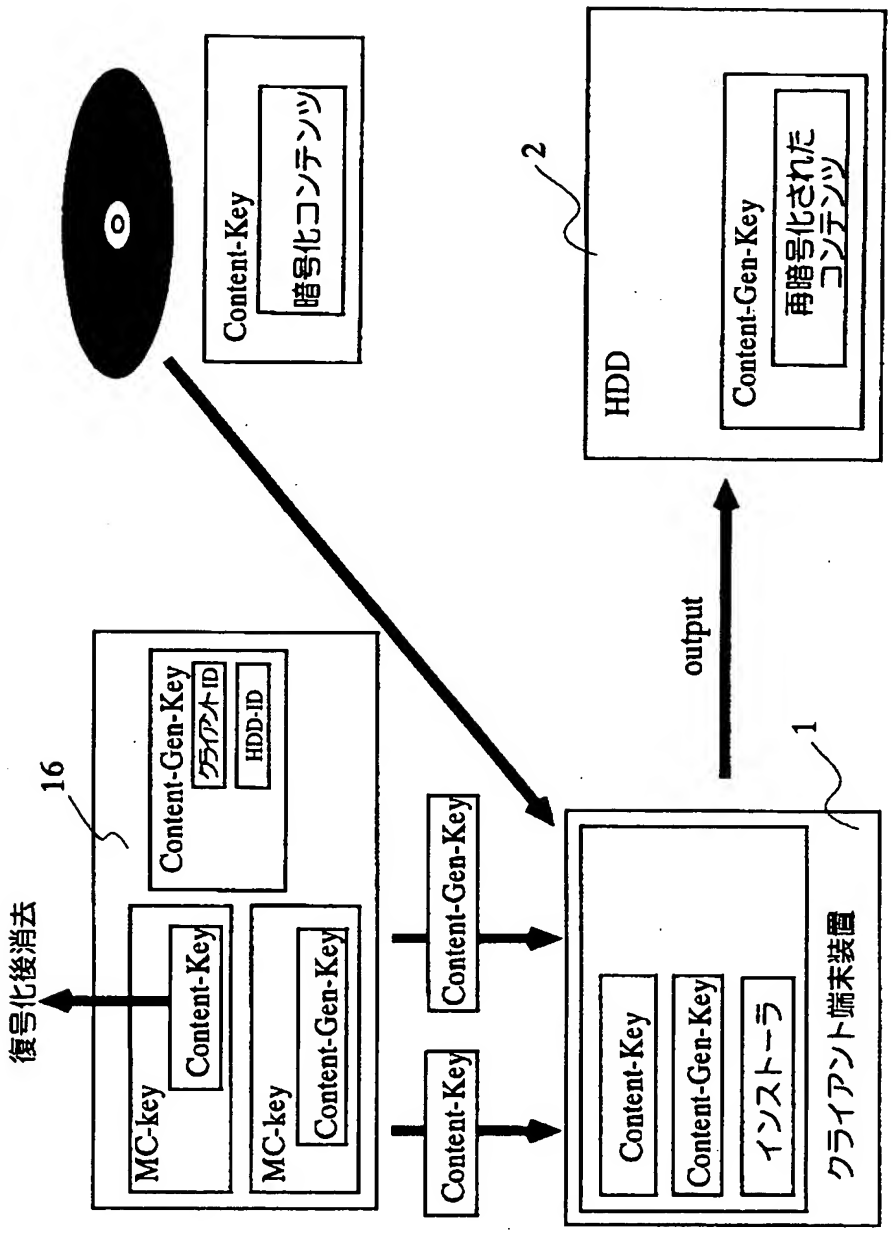
【図８】


media unique ID(MID)
MC－ＩＤ
Content-Key
Encrypted Digital Content
MC-key
UserID
MC-key
mediauniqueID(MID)
システムサーバ装置
1
MC-key
Content-Key
クライアント端末装置
HDD
あらかじめ登録されたMC-Keyで暗号化されたContent-Keyリスト
MC-key
Content-Key
2
16
User ID
media unique ID (MID)
MC－ＩＤ
クライアントID
HDD－ＩＤ
MC-key
Content-Gen-Key
MC-key
Content-Key
Content-Gen-Key
クライアントID
HDD－ＩＤ
MC-key
Content-Gen-Key
チェック
インストールflag→ON
Content-Gen-Key
クライアントID
HDD－ＩＤ
既にインストール済みのMIDリスト
ユーザエントリ情報
4
Memorycard

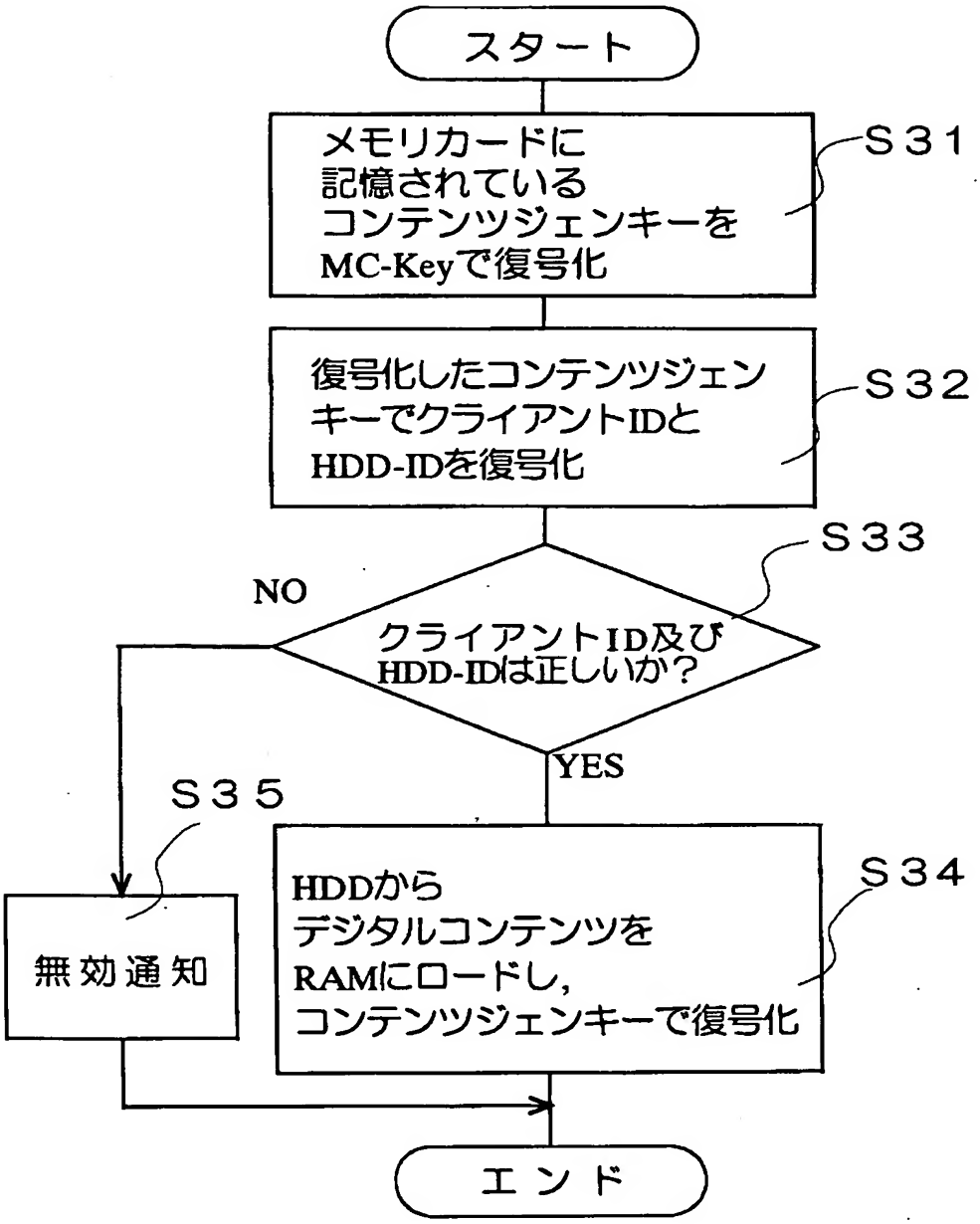
【図９】


スタート
MC-Keyに基づいて
コンテンツキーと
コンテンツジェンキーを
復号化してRAMに記憶
S21
コンテンツジェンキーに基づいて
クライアントIDとHDD-ID
を復号化し照合
S22
S23
NO
クライアントID及び
HDD-IDは正しいか？
YES
S28
無効通知
デジタルコンテンツをコンテンツ
キーで復号化しながら
コンテンツジェンキーで
再暗号化してHDDにコピー
S24
コンテンツジェンキーで
再暗号化された
デジタルコンテンツを保存
S25
S26
コピー完了？
NO
YES
S27
メモリカードの
コンテンツキーを削除
エンド

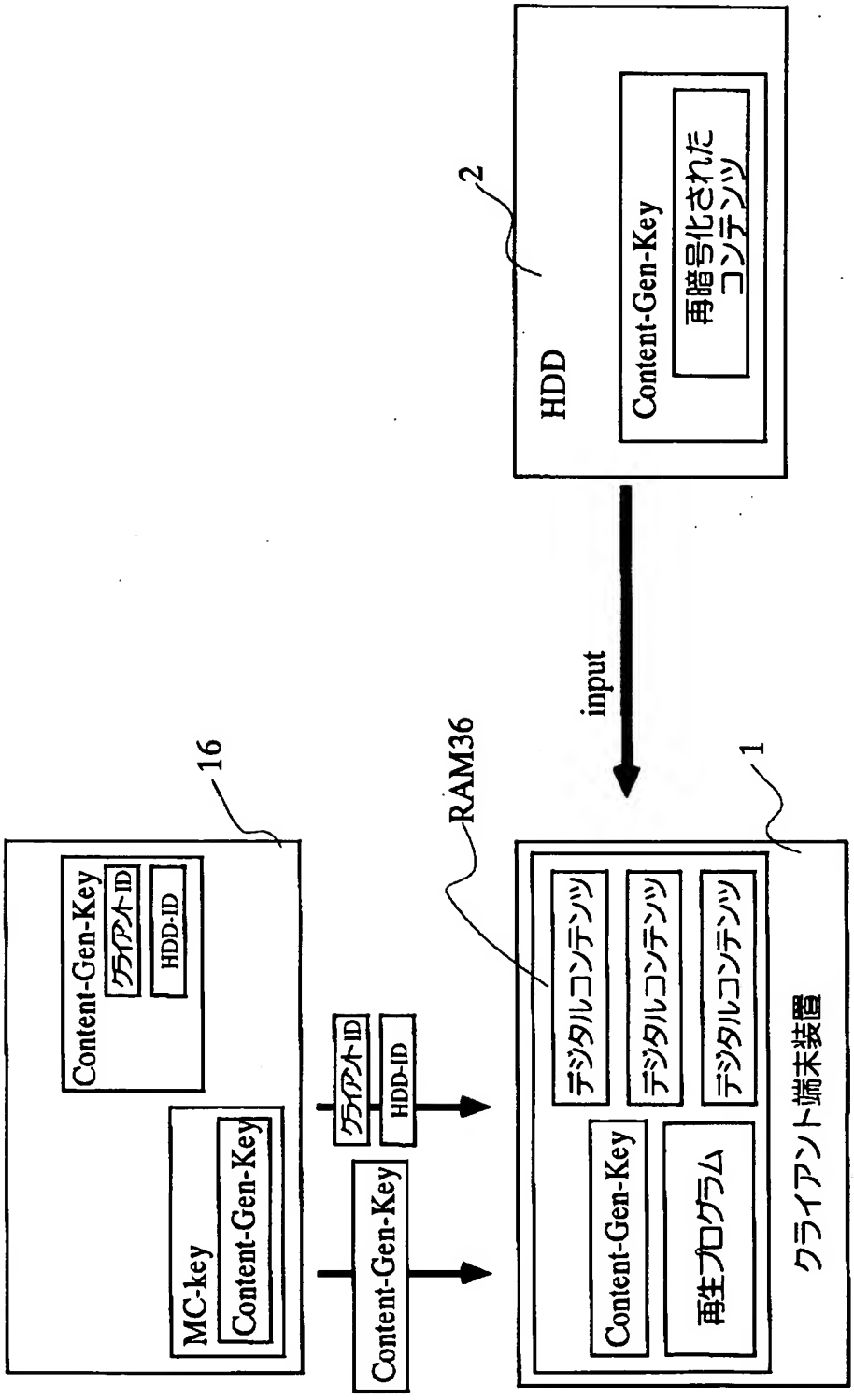
【図１０】


Content-Key
暗号化コンテンツ
2
HDD
Content-Gen-Key
再暗号化されたコンテンツ
output
1
クライアント端末装置
Content-Key
Content-Gen-Key
インストーラ
Content-Key
Content-Gen-Key
16
Content-Gen-Key
クライアントID
HDD-ID
MC-key
Content-Key
MC-key
Content-Gen-Key
復号化後消去

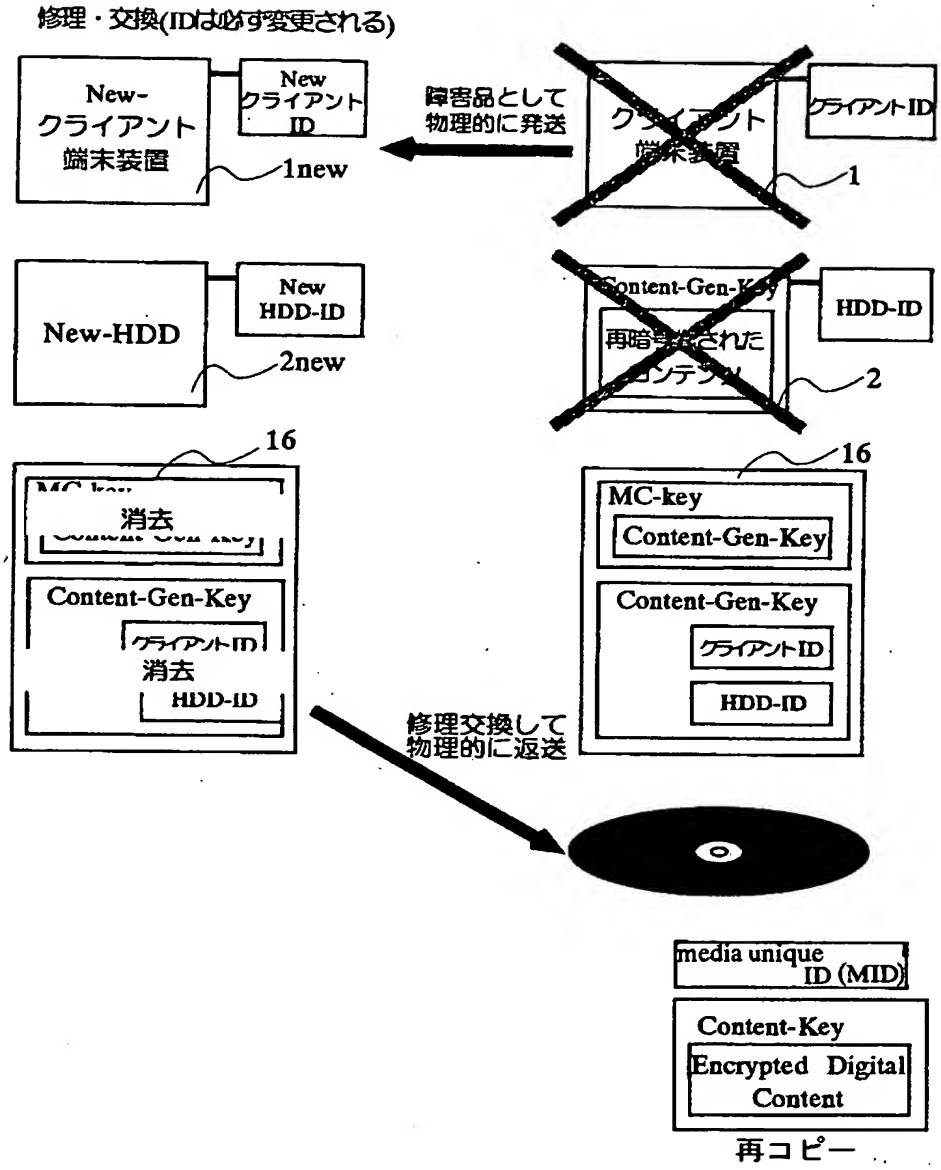
【図１１】


スタート
メモリカードに
記憶されている
コンテンツジェンキーを
MC-Keyで復号化
S31
復号化したコンテンツジェン
キーでクライアントIDと
HDD-IDを復号化
S32
S33
NO
クライアントID及び
HDD-IDは正しいか？
YES
S35
無効通知
HDDから
デジタルコンテンツを
RAMにロードし，
コンテンツジェンキーで復号化
S34
エンド

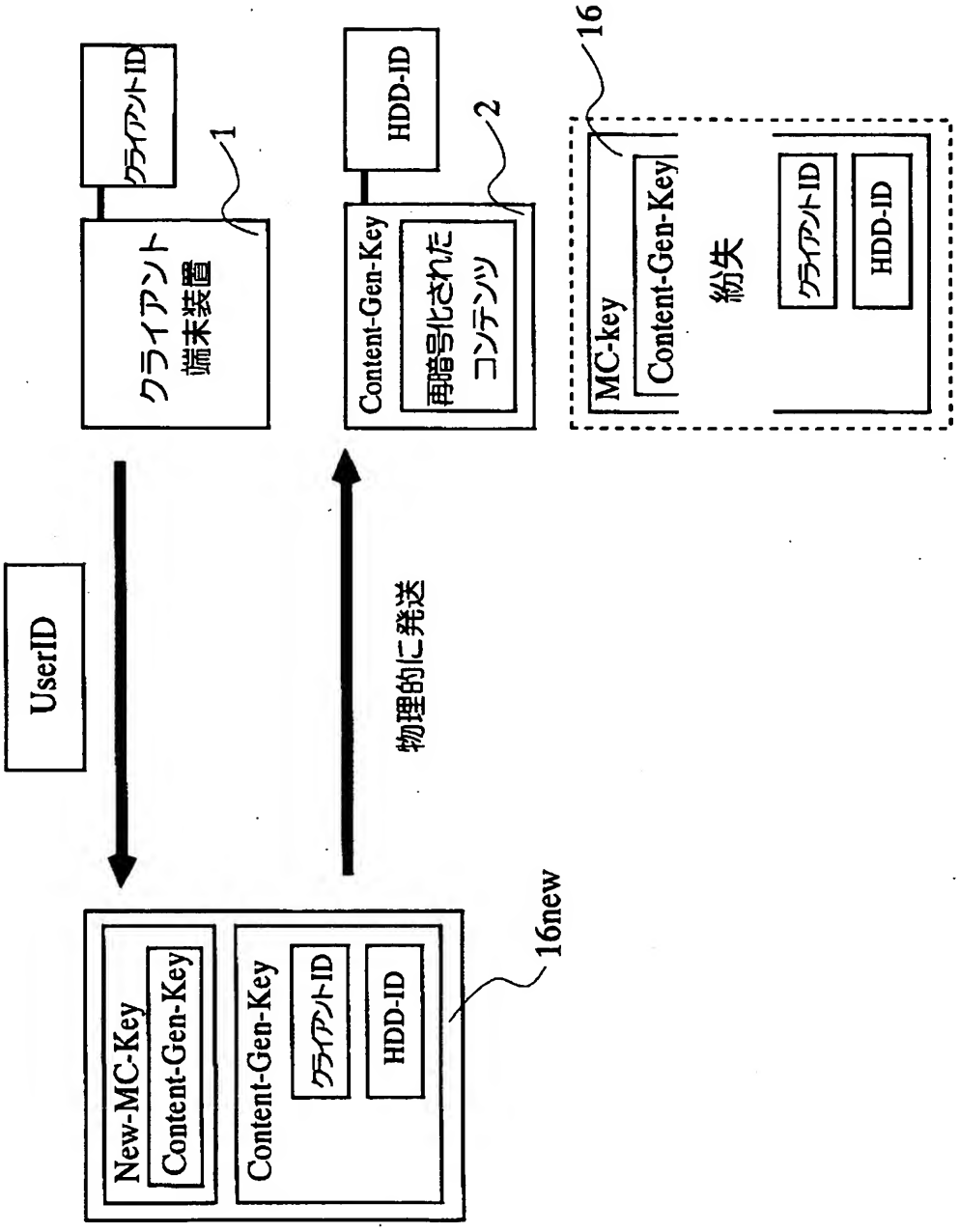
【図１２】


2
HDD
Content-Gen-Key
再暗号化されたコンテンツ
input
RAM36
1
16
Content-Gen-Key
クライアントID
HDD-ID
MC-key
Content-Gen-Key
クライアントID
HDD-ID
Content-Gen-Key
デジタルコンテンツ
デジタルコンテンツ
デジタルコンテンツ
Content-Gen-Key
再生プログラム
クライアント端末装置

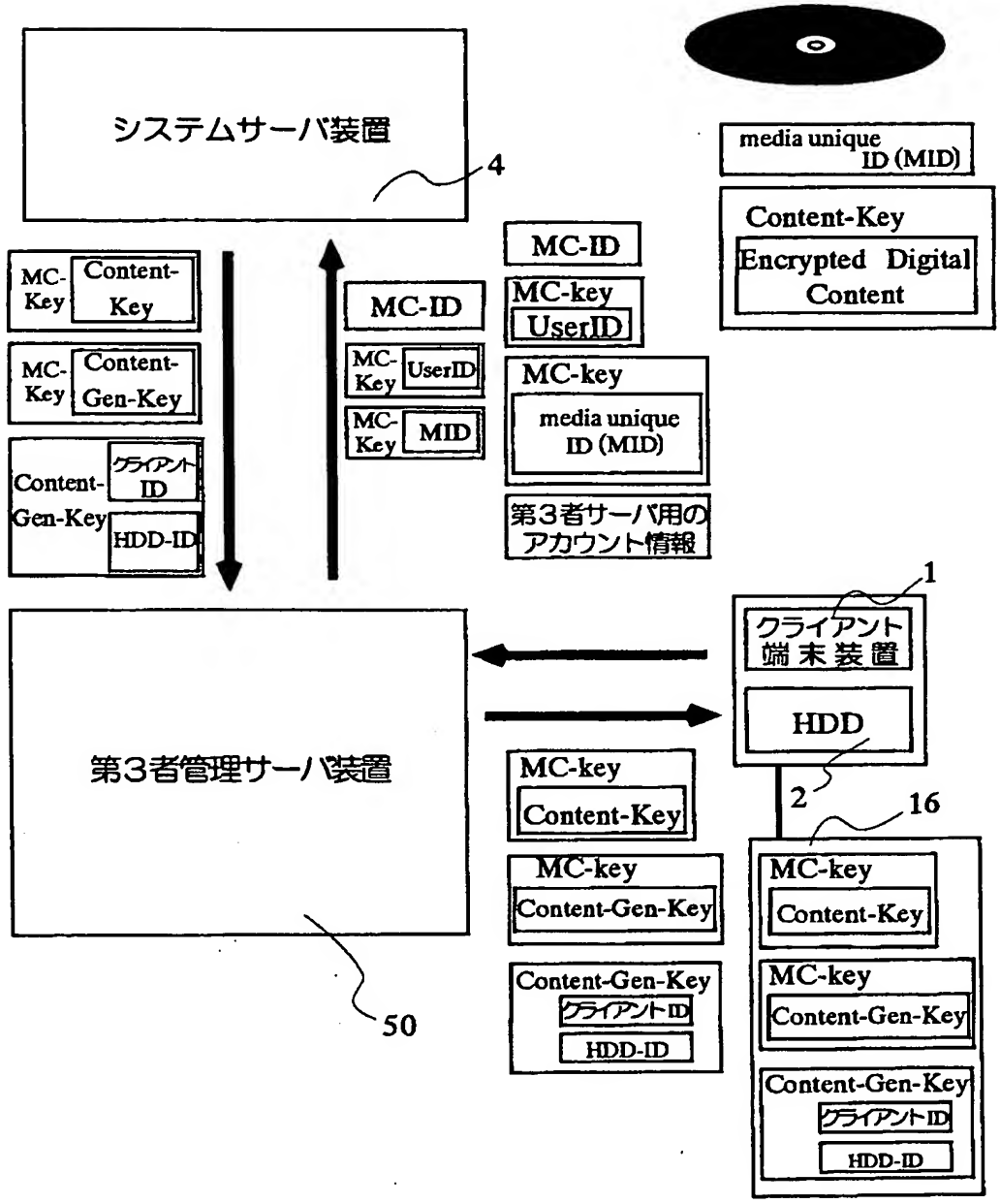
【図１３】


修理・交換(IDは必ず変更される)
New-
クライアント
端末装置
New
クライアント
ID
1new
障害品として
物理的に発送
クライアントID
1
New-HDD
New
HDD-ID
2new
HDD-ID
2
16
消去
Content-Gen-Key
クライアントID
消去
HDD-ID
16
MC-key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
修理交換して
物理的に返送
media unique
ID (MID)
Content-Key
Encrypted Digital
Content
再コピー

【図１４】


クライアントID
1
クライアント
端末装置
HDD-ID
2
Content-Gen-Key
再暗号化された
コンテンツ
16
MC-key
Content-Gen-Key
紛失
クライアントID
HDD-ID
UserID
物理的に発送
New-MC-Key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
16new

【図１５】


システムサーバ装置
4
media unique ID (MID)
Content-Key
Encrypted Digital Content
MC-ID
MC-key
UserID
MC-key
media unique ID (MID)
第3者サーバ用のアカウント情報
MC-Key
Content-Key
MC-Key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
MC-ID
MC-Key
UserID
MC-Key
MID
1
クライアント端末装置
HDD
2
16
第3者管理サーバ装置
50
MC-key
Content-Key
MC-key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID
MC-key
Content-Key
MC-key
Content-Gen-Key
Content-Gen-Key
クライアントID
HDD-ID

【書類名】　　要約書

【要約】

【課題】　コンテンツの不正コピーを防止する。

【解決手段】　各光ディスク毎にＩＤ（MID）を付すと共に、コンテンツをContent-Keyで暗号化して記録しておく。システムサーバ装置は、ユーザが所有するクライアント端末装置のクライアントＩＤ，ＨＤＤのHDD-ID、及びメモリカードのMC-ID等をユーザエントリ情報として管理する。ユーザはコンテンツのコピーを行う際に、光ディスクのMIDと共にMC-IDをシステムサーバ装置に送信する。システムサーバ装置は、MC-IDをユーザエントリ情報と照合してユーザを特定し、コンテンツの暗号化の際に用いたContent-Keyを返送する。ユーザ側では、この返送されたContent-Keyを用いて光ディスクに記録されているコンテンツを復号化しＨＤＤにコピーする。記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーが許可されるため、コンテンツの不正コピーを防止することができる。

【選択図】　図８

出　願　人　履　歴　情　報

識別番号　　〔３９５０１５３１９〕

１．変更年月日　　１９９７年　３月３１日
［変更理由］　住所変更
住　所　東京都港区赤坂７－１－１
氏　名　株式会社ソニー・コンピュータエンタテインメント